Risk Management Policy

Asylum Research & Global Assistance

Preamble

Asylum Research & Global Assistance operates in environments defined by **geopolitical instability, legal complexity, humanitarian urgency, operational volatility, and reputational sensitivity**. The nature of the Organization's work necessarily requires engagement with jurisdictions, institutions, partners, beneficiaries, service providers, and stakeholders whose conditions, interests, and obligations may change rapidly and without warning. In such circumstances, risk cannot be treated as an incidental concern; it must be addressed as a **core function of governance, operational integrity, and institutional survival**.

This Policy establishes a **comprehensive, disciplined, and enforceable framework** for the identification, assessment, treatment, monitoring, and reporting of risk. Its purpose is to ensure that risk is managed not through assumption, improvisation, or convenience, but through **method, evidence, accountability, and continuous oversight**. The Organization recognizes that effective risk management is not merely a matter of administrative prudence; it is an expression of **professional responsibility, ethical seriousness, and strategic discipline**. Every decision taken by or on behalf of the Organization shall therefore be informed by an honest assessment of the consequences, limitations, exposures, and obligations arising from that decision.

The Organization affirms that **risk tolerance is not unlimited**. No operational objective, external request, contractual arrangement, donor expectation, or strategic ambition shall justify the neglect of legal compliance, the compromise of human dignity, the abandonment of duty of care, the misuse of authority, or the concealment of material risk. **Where risk is unavoidable, it must be understood; where it is manageable, it must be controlled; where it is unacceptable, it must be refused.** This principle applies equally to strategic planning, field operations, data handling, procurement, partnerships, financial stewardship, safeguarding obligations, and emergency response.

This Policy further reflects the Organization's commitment to **lawful conduct, moral integrity, operational resilience, and institutional continuity**. It requires that all personnel act with vigilance, candor, and responsibility, and that all departments maintain the capacity to anticipate, detect, and respond to threats before they become failures. The Organization does not regard risk management as a theoretical exercise; it regards it as a practical necessity and a **non-negotiable standard of professional conduct**.

Accordingly, this Policy shall guide the Organization in preserving continuity of service, protecting personnel and beneficiaries, safeguarding assets and information, maintaining compliance with applicable legal and regulatory obligations, and ensuring that the Organization

remains capable of fulfilling its mission under adverse conditions. **Risk management is therefore an affirmative duty, a leadership obligation, and a condition of organizational legitimacy.**

Policy Statement

The Organization shall maintain a **structured risk management system** designed to identify, evaluate, prioritize, mitigate, and review risks across all areas of activity. Risk management shall be integrated into governance, planning, procurement, staffing, partnerships, field deployment, information security, financial controls, and crisis response. No major decision shall be taken without consideration of its foreseeable risks and the corresponding mitigation measures.

The Organization shall adopt a **zero-tolerance approach to concealment, negligence, fraud, corruption, deliberate non-compliance, and reckless disregard for foreseeable harm**. All personnel are required to act in good faith, to escalate risks promptly, to preserve evidence where relevant, and to cooperate fully with internal review and corrective action processes. Failure to report a known or reasonably foreseeable risk may itself constitute a breach of duty.

Risk Management Principles

The Organization's approach to risk management shall be governed by the following principles:

1. Proportionality and Precision. Risk controls shall be proportionate to the seriousness, likelihood, and consequences of the relevant exposure, but they shall never be superficial where the stakes are substantial. The Organization shall distinguish between tolerable risk, manageable risk, and unacceptable risk with rigor and without sentimentality.

2. Accountability and Transparency. Every material risk must have a clearly identified owner, a documented assessment, and a designated response plan. Ambiguity in responsibility is itself a governance failure.

3. Prevention Before Reaction. The Organization shall prioritize anticipation and prevention over crisis response. Early detection, early reporting, and timely mitigation are mandatory institutional expectations.

4. Legal and Ethical Compliance. No risk treatment measure may be implemented in a manner that violates applicable law, undermines safeguarding, compromises human rights, or erodes the Organization's ethical obligations. **Compliance is not optional and ethics are not negotiable.**

5. Continuity and Resilience. The Organization shall maintain operational continuity through redundancy, preparedness, contingency planning, and the capacity to adapt under pressure without abandoning standards.

Scope of Application

This Policy applies to **all directors, officers, employees, consultants, volunteers, contractors, agents, and representatives** of the Organization, regardless of location, contractual status, or functional role. It applies to all programs, projects, field activities,

partnerships, fundraising efforts, logistics operations, digital systems, data repositories, financial activities, and external engagements conducted in the name of or on behalf of the Organization.

No person acting for the Organization is exempt from this Policy. No operational urgency excuses noncompliance. No external relationship overrides the duty to manage risk responsibly. **The reach of this Policy is universal within the Organization's sphere of action.**

Risk Governance and Responsibility

The Board of Directors and senior leadership bear the ultimate responsibility for ensuring that risk is properly governed, reviewed, and resourced. They shall set the Organization's overall risk appetite, approve material risk frameworks, receive escalation of significant exposures, and ensure that corrective action is taken where necessary. Management shall be responsible for implementing risk controls in practice, maintaining accurate documentation, and ensuring that risk considerations are embedded in operational decision-making.

Every unit, function, and individual with decision-making authority shall maintain appropriate awareness of the risks associated with its activities. **Risk ownership is a duty, not a formality.** Where a risk exceeds the authority or capacity of a local unit, it must be escalated without delay to the relevant senior authority. The Organization shall not permit a culture in which material risks are minimized for convenience, ignored for optimism, or concealed to avoid scrutiny.

Risk Identification, Assessment, and Treatment

The Organization shall identify risks through continuous review of operational, legal, financial, security, technological, reputational, safeguarding, and environmental factors. Risk identification shall be proactive, not reactive, and shall include both internal vulnerabilities and external developments that may affect the Organization's ability to function or fulfill its mission.

Each identified risk shall be assessed according to its **likelihood, impact, urgency, and potential persistence**, taking into account the vulnerability of affected persons, the scale of possible harm, and the Organization's capacity to respond. Assessments shall be documented with sufficient clarity to support informed decision-making. The Organization shall not rely on vague impressions, informal assurances, or unsupported optimism where objective evaluation is required.

Where a risk is accepted, the basis for acceptance must be explicitly recorded and approved at the appropriate level. Where a risk is mitigated, the measures chosen must be practical, monitorable, and capable of reducing exposure to an acceptable level. Where a risk cannot be adequately reduced, the Organization shall consider suspension, redesign, transfer, limitation, or termination of the relevant activity. **No activity shall continue merely because it is already underway.**

Monitoring, Reporting, and Review

Risk management is a continuous obligation. Risks shall be monitored on an ongoing basis, with particular attention to changes in operational context, legal obligations, partner reliability,

security conditions, public perception, and financial exposure. Material incidents, near misses, control failures, and adverse trends shall be recorded and reviewed to identify lessons learned and to prevent recurrence.

Significant risks shall be escalated promptly and without distortion. Reporting must be **accurate, complete, timely, and candid**. Misleading reports, selective disclosure, and delayed escalation undermine institutional integrity and may expose the Organization and its stakeholders to preventable harm. Reviews shall be conducted periodically and whenever circumstances materially change, including after incidents, audits, field shocks, regulatory developments, or strategic shifts.

Commitment to Institutional Integrity

The Organization recognizes that a sound risk management framework is inseparable from **integrity, discipline, and trustworthiness**. It shall therefore maintain controls and procedures that discourage misconduct, detect irregularities, and support corrective action where failures occur. The Organization will not tolerate behavior that places expediency above duty, convenience above compliance, or silence above truth. **Professionalism requires vigilance; leadership requires accountability; integrity requires decisive action.**

This Policy shall be interpreted and applied in a manner consistent with the Organization's mission, applicable law, and the highest standards of responsible governance. It is intended to protect not only the Organization's institutional interests, but also the safety, dignity, and lawful rights of those whom the Organization serves and those with whom it works.

I. RISK CATEGORIES

ASYLUM RESEARCH & GLOBAL ASSISTANCE recognizes that risk is an inherent and unavoidable condition of operating in complex, high-volatility, and often legally sensitive environments. The Organization therefore treats risk identification, prevention, mitigation, escalation, and documented review as **fundamental governance obligations**, not as discretionary administrative functions. Each risk category below must be understood as interdependent; a failure in one domain may rapidly intensify exposure in another. Accordingly, the Organization maintains a disciplined approach grounded in **legal compliance, fiduciary responsibility, operational resilience, and ethical non-negotiability**. No risk may be minimized, normalized, or tolerated where it threatens the Organization's mandate, beneficiaries, staff, assets, partners, or legal standing.

A. Strategic Risks

Strategic risk refers to the possibility that the Organization's long-term direction, institutional credibility, or programmatic relevance may be undermined by internal misalignment or external change. The most significant strategic threat is **mission drift**, meaning the gradual or abrupt departure of activities, partnerships, or geographic priorities from the Organization's founding purpose, humanitarian principles, and internationally recognized development objectives. The Organization must ensure that its programs remain demonstrably aligned with relevant **Sustainable Development Goals**, protection standards, and governance expectations, and that

any shift in mandate is deliberate, documented, reviewed at leadership level, and defensible in both ethical and legal terms. Strategic failure can also arise where governance reforms, political transitions, regulatory changes, or institutional restructuring alter the Organization's operating space, mandate assumptions, or access to communities. Such changes must be monitored continuously, because an organization that fails to adapt lawfully and prudently may lose legitimacy, funding, and operational authority.

A second major strategic exposure is **funding concentration and market dependence**. Overreliance on a limited number of donors, funding streams, or grant cycles creates structural vulnerability, especially where grant decisions are delayed, revised, or suspended due to political developments, budget contractions, or donor reprioritization. The Organization must recognize that delayed funding is not merely an administrative inconvenience; it can trigger service disruption, staffing instability, contractual breach, and reputational harm. Economic downturns, inflationary shocks, sovereign instability, and reduced philanthropic appetite may also weaken funding predictability. For this reason, strategic planning must include realistic assumptions regarding donor behavior, funding diversification, reserve adequacy, and continuity of essential programs.

Strategic risk further includes **reputational exposure**, particularly where the Organization is associated, whether directly or indirectly, with controversial entities, compromised partners, politicized actors, or operational decisions that may reasonably be perceived as inconsistent with humanitarian integrity. Public criticism, adverse media coverage, or allegations of bias, mismanagement, or improper affiliation can materially damage trust and impair access to beneficiaries, donors, regulators, and host authorities. The Organization must therefore exercise rigorous partner due diligence, communications discipline, and ethical screening. **Reputation is not cosmetic; it is an operational asset and a legal safeguard.** Once impaired, it can compromise grant eligibility, registration status, stakeholder confidence, and the Organization's ability to act with authority in the field.

B. Operational Risks

Operational risk concerns the possibility that the Organization's day-to-day functions, service delivery mechanisms, personnel continuity, or technology systems may fail, degrade, or become inaccessible. In humanitarian and research contexts, operational risk is heightened by insecurity, displacement, environmental instability, weak infrastructure, and rapidly changing ground conditions. The Organization must therefore maintain procedures that are not only efficient but also **resilient under stress**, with clear lines of accountability, contingency planning, and documented escalation pathways. Operational preparedness is a duty of care issue, a continuity issue, and in many settings a legal exposure issue.

A primary operational vulnerability is **staffing risk**, particularly **key-person dependency**, talent retention failure, burnout, and insufficient succession planning. Where critical knowledge, relationships, approvals, or technical capacity are concentrated in a small number of individuals, the Organization becomes fragile and exposed to interruption if those individuals resign, become unavailable, or are otherwise unable to perform. Humanitarian and research environments frequently produce elevated stress, emotional fatigue, exposure to trauma, and chronic overload.

The Organization must treat burnout as a foreseeable operational risk requiring active management through workload controls, supervision, psychosocial support, rest cycles, and role redundancy. Failure to do so may lead to unsafe performance, ethical lapses, turnover, and reduced institutional reliability.

Operational risk also includes **service delivery disruption** caused by conflict, civil unrest, natural disasters, pandemics, transport disruption, access denial, supply chain collapse, or communications failure. The Organization must assume that field conditions may deteriorate without warning and that program continuity may depend on rapid adaptation, remote coordination, alternative routing, or temporary suspension. The Organization's obligation is not to guarantee uninterrupted operations in hostile conditions, but to demonstrate **reasonable foresight, preparedness, and proportionate response**. Where interruption occurs, the Organization must prioritize staff safety, beneficiary protection, data preservation, and lawful suspension or modification of activities.

A further operational exposure is **technology and information systems failure**, including system outages, cyberattacks, unauthorized access, corruption of data, loss of devices, and inadequate backup architecture. The Organization's operational and legal risk increases materially where sensitive personal data, beneficiary records, research files, financial records, or partner information are stored without adequate security controls. Cybersecurity must therefore be understood as a governance matter, not merely an IT function. The Organization must maintain access controls, authentication standards, backup and recovery protocols, device management, encryption where appropriate, and incident response procedures. **Data loss, data leakage, or system compromise can produce legal liability, reputational damage, donor concern, and direct harm to vulnerable persons.**

C. Compliance Risks

Compliance risk arises where the Organization, its staff, contractors, agents, or partners may fail to comply with applicable laws, regulations, administrative requirements, sanctions regimes, labor obligations, tax rules, or internal policy commitments. Compliance must be treated as a core institutional obligation because legal non-compliance can result in fines, license suspension, de-registration, asset seizure, investigation, civil claims, criminal exposure, and severe reputational damage. The Organization shall operate on the principle that **ignorance of applicable law is not a defense** and that "informal practice" can never override binding legal obligations.

A central compliance exposure is **regulatory change**. Local law may change with little notice, particularly in relation to NGO registration, foreign funding controls, reporting duties, procurement restrictions, tax treatment, data protection, import/export permissions, and operational authorization. The Organization must continuously monitor the legal environment in each jurisdiction of activity and ensure that registration status, reporting schedules, and licensing obligations remain current. Where legal conditions change, the Organization must act promptly to reassess operations, suspend non-compliant activity where necessary, and obtain appropriate legal guidance. Delayed action in response to legal change can convert a manageable administrative issue into a substantive violation.

The Organization also faces significant **sanctions and restricted-party risk**, including inadvertent dealings with sanctioned individuals, prohibited entities, front organizations, or intermediaries acting on behalf of restricted parties. This risk extends to donations, procurement, subcontracting, logistics, service delivery, and partner engagement. The Organization must maintain robust screening procedures, escalation protocols, recordkeeping standards, and approval controls. **Unintentional exposure is still exposure**; the absence of bad intent does not eliminate legal and reputational consequences. In this domain, disciplined due diligence is not optional, and tolerance for ambiguity must be extremely limited.

Compliance risk further includes **labor and human resources violations**, such as unlawful termination, wage underpayment, excessive working hours, discrimination, harassment, retaliation, unsafe working conditions, or breach of contractual entitlements. These matters are not merely internal personnel concerns; they are legal and moral obligations that directly reflect the Organization's integrity. The Organization must ensure that employment practices are lawful, documented, non-discriminatory, and consistent with applicable labor standards and internal policy. Where disputes arise, they must be addressed promptly, fairly, and with appropriate documentation, without favoritism, concealment, or retaliatory conduct.

D. Financial Risks

Financial risk concerns the possibility that the Organization may suffer losses, liquidity stress, asset misappropriation, exchange-rate volatility, or weak financial controls that impair stability and accountability. Financial integrity is essential because the Organization is entrusted with resources that are intended to serve public, humanitarian, and research purposes. Any failure in financial stewardship undermines donor confidence, internal discipline, and the Organization's moral legitimacy. The Organization must therefore maintain a strict framework of authorization, segregation of duties, oversight, reconciliation, and auditability.

A principal financial exposure is **fraud**, including embezzlement, false invoicing, procurement manipulation, payroll abuse, forged documentation, ghost vendors, and unauthorized diversion of assets. Fraud risk is elevated where controls are weak, oversight is fragmented, field access is limited, emergency spending is frequent, or one individual exercises excessive discretion. The Organization must recognize that fraud is not only a financial loss event; it is a breach of trust and, in many cases, a serious legal violation. Prevention requires strong approvals, vendor verification, independent review, documented expenditure support, exception monitoring, and protected reporting channels. **Zero tolerance for financial dishonesty is a governing principle.**

The Organization must also manage **liquidity risk**, meaning the possibility that cash on hand, committed funding, and receivable timing may be insufficient to meet payroll, vendor obligations, program costs, or statutory payments when due. Timing mismatches between expenses and incoming funds are especially dangerous in grant-dependent operations. A technically solvent organization may still be unable to function if it lacks timely liquidity. This risk requires active cash flow forecasting, reserve management, payment prioritization, and early escalation where funding delays or cost overruns threaten continuity.

Finally, **currency risk** is a material concern in multi-jurisdiction and multi-currency operations. Exchange rate volatility may materially affect program budgets, purchasing power, salary commitments, transfer values, and reporting accuracy. Where revenues are received in one currency and expenditures are incurred in another, even modest market fluctuations can create significant operational pressure. The Organization must therefore maintain realistic budgeting assumptions, timely conversion strategies, and where appropriate hedging or contingency mechanisms, subject always to legality, prudence, and governance approval. **Financial stewardship requires not only accuracy, but anticipation.**

II. RISK ASSESSMENT METHODOLOGY

A. Probability & Impact Matrix

The risk assessment framework of **ASYLUM RESEARCH & GLOBAL ASSISTANCE** is founded upon a disciplined, transparent, and consistently applied **Probability & Impact Matrix**, designed to ensure that every identified risk is evaluated according to a uniform standard of legal, operational, strategic, and reputational significance. The purpose of this methodology is not merely to classify risk, but to establish a **defensible decision-making structure** that enables the organization to identify, prioritize, escalate, and mitigate threats in a manner that is proportionate, timely, and accountable.

Each risk is assessed across two independent dimensions: **Probability** and **Impact**. **Probability** measures the likelihood that a given event, condition, or failure mode will occur within the relevant assessment period. This measure is assigned on a five-point scale, where **1 signifies a Rare event** and **5 signifies an Almost Certain event**. The score must reflect evidence-based judgment, taking into account historical occurrence, current controls, environmental volatility, regulatory exposure, operational complexity, and any observable indicators of deterioration or escalation. Speculation, convenience, or subjective optimism shall not substitute for reasoned assessment. Where data is incomplete, the organization shall apply conservative judgment and may not minimize risk by assuming the absence of evidence to be evidence of absence.

Impact measures the severity of consequences should the risk materialize. It is likewise assigned on a five-point scale, where **1 denotes Negligible consequence** and **5 denotes Catastrophic consequence**. Impact must be assessed in a comprehensive manner, including but not limited to **human safety, legal liability, regulatory breach, financial loss, operational interruption, data compromise, loss of trust, humanitarian harm, and reputational damage**. In contexts involving vulnerable persons, protected interests, or cross-border assistance activities, the assessment of impact shall be especially rigorous, because the moral and legal consequences of failure may be irreparable. The organization shall not trivialize harm merely because it is indirect, delayed, or difficult to quantify.

The **Risk Score** is determined by the formula **Probability × Impact**, producing a standardized scale from **1 to 25**. This quantitative mechanism is intended to support prioritization, not to reduce professional judgment to arithmetic alone. The score must be interpreted in context, with due consideration of compounding factors, interdependencies, and latent risks that may not be

fully reflected in a numerical result. Accordingly, a low score does not automatically mean a risk is insignificant, and a high score may require immediate operational and legal intervention regardless of whether formal thresholds have been reached.

To ensure consistency of response, risks shall be categorized as follows:

- **Red (16–25): immediate mitigation required**
- **Yellow (9–15): close monitoring and controlled mitigation**
- **Green (1–8): accepted only under active oversight and periodic review**

A **Red** classification indicates a condition of unacceptable exposure requiring immediate corrective action, escalation to the appropriate authority, and the prompt implementation of containment measures. No delay is permissible where the risk presents a credible threat to persons, legal compliance, operational continuity, or institutional integrity. A **Yellow** classification indicates that the risk is material and must be actively monitored through enhanced controls, defined ownership, and scheduled reassessment. Such risks may be tolerated only where there is a documented justification, an identified mitigation pathway, and clear evidence that the organization has neither ignored nor underestimated the exposure. A **Green** classification does not signify the absence of concern; rather, it indicates that the risk is presently manageable within existing controls, subject to continued observation and prompt reclassification if circumstances change.

The matrix shall be applied in a manner that is **consistent, auditable, and resistant to bias**. The organization shall maintain written rationale for all scores assigned, especially where judgment is exercised in borderline or ambiguous cases. This record is essential to demonstrate that assessments were conducted with diligence, fairness, and professional integrity. Where a risk implicates legal obligations, regulatory standards, or duty-of-care responsibilities, the higher severity interpretation shall prevail unless a documented and objectively justified basis exists for a different conclusion.

B. Risk Register

The **Risk Register** is the central and authoritative record of all identified risks, serving as the organization's formal instrument for oversight, traceability, and accountability. It shall function as a living document, not a static inventory, and must reflect the current risk posture of the organization at all times. The register must include, at a minimum, a comprehensive description of each risk, the relevant business area or process affected, the assigned owner, the probability rating, the impact rating, the resulting score, the status of mitigation measures, the review schedule, and the date of last reassessment.

Each risk entry must identify a clearly responsible **risk owner**. Ownership shall not be symbolic or nominal; it must represent real accountability for monitoring the risk, advancing mitigation actions, maintaining evidence of progress, and escalating unresolved issues when necessary. The risk owner is expected to ensure that controls are not merely stated in principle but implemented in practice, tested for effectiveness, and revised where they prove inadequate. Where a risk spans

multiple functions, the organization shall designate a lead owner while preserving cross-functional responsibility and coordination.

The register must also record the **mitigation strategy** associated with each risk. This strategy shall describe the controls already in place, the additional measures required, the target completion timeline, any dependencies, and the residual risk expected after mitigation. The organization shall distinguish clearly between **preventive controls**, **detective controls**, and **corrective controls**, and shall not rely on vague assurances or aspirational language in place of specific action. Every mitigation plan must be proportionate to the gravity of the risk and should be capable of objective verification.

A recorded **review date** must be attached to each risk, and all entries shall be subject to **quarterly updates** as a minimum standard. Quarterly review is the baseline expectation, not the limit of organizational vigilance. Where the threat environment changes materially, where an incident occurs, or where a control fails or is weakened, immediate reassessment shall be required regardless of the next scheduled review date. In addition, the entire register shall undergo a formal **annual re-assessment** to ensure that ratings, controls, and ownership remain aligned with current realities, regulatory developments, and operational experience.

Access to the Risk Register shall be provided to relevant stakeholders through a **secure portal** with appropriate authorization controls, confidentiality protections, and audit logging. Access shall be granted on a need-to-know basis and in accordance with the organization's legal, ethical, and security obligations. The purpose of accessibility is to promote informed governance, not to expose sensitive information indiscriminately. Accordingly, the organization shall preserve the integrity, confidentiality, and evidentiary value of the register while ensuring that stakeholders with legitimate oversight responsibilities can review the information necessary to discharge their duties effectively.

The Risk Register is also a critical mechanism for institutional memory and governance discipline. It enables the organization to demonstrate that risks have been identified, assessed, assigned, monitored, and addressed with due seriousness. It provides documentary evidence that decisions were made responsibly and that no material issue was concealed, deferred without justification, or left without ownership. In this sense, the register is not merely an internal administrative tool; it is a **formal expression of the organization's commitment to lawful conduct, operational prudence, and uncompromising accountability**.

III. RISK MITIGATION STRATEGIES

Risk mitigation is not a discretionary management preference; it is a mandatory governance function designed to preserve human safety, organizational integrity, legal compliance, operational continuity, fiduciary prudence, and reputational credibility. ASYLUM RESEARCH & GLOBAL ASSISTANCE shall apply risk mitigation measures in a manner that is **lawful, proportionate, evidence-based, ethically defensible, and operationally enforceable**. The organization shall not tolerate avoidable exposure where reasonable control is available, and shall not subordinate **human security, legal obligations, or moral responsibility** to convenience, speed, commercial pressure, or political expediency. Every

mitigation decision shall be grounded in documented risk assessment, senior accountability, and continuous review.

A. Avoidance

Avoidance is the highest and most decisive form of risk control and shall be employed whenever a risk cannot be reduced to a tolerable level by reasonable and lawful means. Where the nature, scale, or volatility of the threat creates exposure that is **unmitigable, indeterminate, or incompatible with responsible operations**, ASYLUM RESEARCH & GLOBAL ASSISTANCE shall withdraw, decline, suspend, or refuse involvement. This principle applies particularly to environments affected by active hostilities, uncontrolled criminality, targeted persecution, severe infrastructure collapse, systemic corruption, or any condition in which the organization cannot reasonably assure the safety of personnel, beneficiaries, partners, or assets.

Avoidance also applies where a proposed activity would **conflict with the organization's mission, ethical framework, legal obligations, or public trust**. The organization shall decline programs, partnerships, funding arrangements, or operational requests that would compromise independence, humanitarian neutrality, due process, confidentiality, anti-corruption standards, safeguarding duties, or the dignity and rights of protected persons. **No objective, financial benefit, political advantage, or operational ambition shall justify participation in conduct that is unlawful, morally compromised, or incompatible with the organization's standards.** Where avoidance is warranted, the decision shall be recorded with clear reasons, risk evidence, approving authority, and any residual obligations, including duty-of-care measures for staff disengagement and partner notification. Avoidance is not failure; it is **responsible refusal in the interest of lawful and principled conduct**.

B. Reduction

Where a risk cannot be eliminated entirely, the organization shall implement **risk reduction measures that measurably decrease likelihood, severity, and duration of harm**. Reduction must be systematic, not symbolic. It shall include internal controls, operational discipline, supervision, and verification mechanisms designed to detect failure early and prevent escalation. Core controls shall include **segregation of duties**, dual or multi-level approvals for sensitive actions, secure recordkeeping, access restrictions, conflict-of-interest checks, incident reporting channels, and real-time monitoring where exposure is material. These controls shall be calibrated to the sensitivity of the activity, the value of assets involved, and the vulnerability of persons affected. **No critical process shall rely solely on trust, habit, or informal oversight** where formal control is reasonably practicable.

Reduction also requires **diversification as a resilience doctrine**. The organization shall avoid single points of failure by maintaining multiple funding sources where feasible, broadening geographic and logistical presence through distributed capacity, and ensuring that knowledge, decision-making, and technical expertise are not concentrated in one individual, office, donor, supplier, or jurisdiction. Diversification must be deliberate and strategic: funding concentration, procurement dependency, technology monoculture, and personnel overreliance are

all material risk amplifiers. In addition, the organization shall invest in **cross-trained skill sets**, succession readiness, vendor redundancy, secure communications, and contingency operating models to preserve continuity under stress. Reduction is effective only when controls are actively tested, corrected, and audited. Accordingly, risk owners shall measure control performance, document deficiencies, and escalate material weaknesses without delay. **A control that exists only on paper is not a control; it is an unverified assumption.**

C. Transfer

Risk transfer is appropriate when exposure can be shifted, in whole or in part, to another party through lawful contractual, financial, or insurance mechanisms, while recognizing that **transfer does not eliminate accountability**. The organization shall use transfer prudently and only after confirming that the residual risk remains within acceptable limits and that the counterparty is capable, solvent, and contractually bound to perform. Insurance shall be maintained where commercially and operationally justified, including **general liability, directors' and officers' liability, cyber liability, property coverage, professional indemnity where applicable, and any region-specific or activity-specific protection necessary to sustain operations**. Insurance policies shall be reviewed for exclusions, territorial limitations, claims conditions, notification requirements, and gaps that could leave the organization exposed despite apparent coverage. **Coverage without enforceability is not protection**.

Outsourcing may also serve as a transfer mechanism where specialized third-party managed services provide greater reliability, expertise, or scalability than internal delivery. However, outsourcing shall never be treated as abdication. Every third-party arrangement shall be governed by **clear service-level agreements, confidentiality obligations, data protection clauses, performance standards, audit rights, incident notification duties, termination rights, and compliance warranties**. The organization shall perform due diligence before engagement and ongoing oversight thereafter, including security review, financial assessment, sanctions screening where relevant, and integrity checks commensurate with the risk profile. Sensitive functions such as information systems, logistics, safeguarding support, and regulated processing shall not be delegated without explicit review of operational dependencies and failure consequences. **A third party may perform the function, but the organization remains responsible for the outcome.** Transfer is therefore a lawful instrument of resilience, not a substitute for governance, ethics, or vigilance.

D. Acceptance

Risk acceptance shall apply only where a residual risk is **low, understood, monitored, and proportionate to the value of the activity concerned**, and where additional mitigation would be unreasonable, ineffective, or disproportionate to the harm avoided. Acceptance is a conscious governance decision, not passivity and not neglect. The organization shall accept risk only after it has been identified, assessed, recorded, and reviewed by the appropriate authority. Accepted risks must have a defined rationale, a designated owner, a review schedule, and clearly stated triggers for escalation. **Acceptance without monitoring is mismanagement; acceptance with disciplined oversight is strategic prudence**.

Low-level or low-probability items may be monitored without immediate intervention, provided that the organization retains awareness of trends, warning indicators, and changes in context. Nevertheless, the principle of acceptance shall never be used to justify indifference toward foreseeable harm, especially where vulnerable persons, protected data, fiduciary resources, or legal compliance are implicated. For strategic risks that cannot be avoided, reduced, or transferred at acceptable cost, the organization shall maintain **contingency reserves, continuity plans, alternate pathways, and decision thresholds** sufficient to preserve operational stability. Such reserves may include financial buffers, standby capacity, emergency procurement authority, backup suppliers, and crisis escalation procedures. Acceptance must always be paired with readiness: **the organization may choose to tolerate a risk, but it may never choose to be unprepared for its realization**.

IV. BUSINESS CONTINUITY PLANNING

ASYLUM RESEARCH & GLOBAL ASSISTANCE shall maintain and continuously improve a comprehensive **Business Continuity Planning framework** designed to ensure the uninterrupted, lawful, and operationally resilient delivery of critical services under conditions of disruption, whether arising from natural catastrophe, infrastructure failure, public health emergency, cyber incident, civil unrest, supply chain interruption, personnel unavailability, or any other event reasonably capable of impairing ordinary business operations. The organization shall treat continuity planning not as an administrative formality, but as a **mandatory governance function**, integral to the protection of clients, personnel, records, funds, operational integrity, and institutional credibility.

1. Alternate Work Facilities and Operational Redundancy

The organization shall identify, validate, and maintain **alternate work facilities** for all major operational hubs and mission-critical functions, including remote work arrangements, secondary office locations, temporary relocation options, and digital work continuity solutions where physical occupancy becomes impracticable or unsafe. Such facilities shall be selected on the basis of operational suitability, communications reliability, data access capability, security requirements, and the ability to sustain essential services without material degradation in quality or compliance. The continuity model shall ensure that no single point of physical failure can wholly disable critical operations. Each designated alternate site shall be supported by documented access protocols, assignment of responsible personnel, communication procedures, and minimum technical requirements necessary to restore essential functions within a reasonable recovery timeframe. ASYLUM RESEARCH & GLOBAL ASSISTANCE shall ensure that these arrangements are reviewed periodically and updated to reflect changes in organizational structure, staffing, technology, service demand, and risk exposure. **Continuity of operations shall be treated as a standing institutional obligation, not a discretionary contingency.**

2. Documentation of Key Processes and Step-by-Step Recovery Procedures

All key business, administrative, financial, case-related, research-related, and client-support processes shall be **documented in a clear, step-by-step format** sufficient to permit timely continuation by authorized personnel even in the absence of the primary process owner. Documentation shall identify the process objective, sequence of actions, required inputs, system

dependencies, responsible roles, internal controls, escalation triggers, approval requirements, and any legal, regulatory, or ethical constraints applicable to performance of the process. Special attention shall be given to functions whose interruption would cause immediate prejudice to clients, compromise deadlines, impair evidence handling, disrupt secure communications, or expose the organization to regulatory or contractual breach. The documentation shall be written with sufficient precision to permit practical execution under emergency conditions, and shall be stored in secure, accessible, and redundant formats to ensure availability when standard systems are impaired. Each critical procedure shall be subject to periodic review for accuracy, completeness, and operational relevance, with revisions documented and approved in accordance with internal governance requirements. **No essential process shall remain dependent solely upon undocumented institutional memory or informal practice.**

3. Emergency Funding and Financial Resilience

The organization shall maintain an **emergency reserve fund equal to no less than three months of operating expenses**, calculated on the basis of reasonably anticipated recurring expenditures necessary to preserve essential operations, including payroll obligations, facility costs, communication services, technology support, contractual commitments, and other indispensable operating outlays. This reserve shall be preserved in a manner that ensures both availability and prudent stewardship, with internal controls designed to prevent unauthorized use, commingling, or diversion for non-emergency purposes. Access to emergency funds shall be governed by clear authorization thresholds, documented decision-making criteria, and oversight mechanisms sufficient to ensure that any deployment of reserve resources is necessary, proportionate, and directly connected to continuity preservation. The organization shall regard financial preparedness as a core element of institutional responsibility, recognizing that operational continuity cannot be sustained without immediate access to liquid resources in periods of disruption. **Financial resilience is a legal and ethical condition of continuity, not an optional safeguard.**

4. Annual Business Continuity Drills, Review, and Corrective Action

The organization shall conduct **formal business continuity drills at least annually**, and more frequently where material changes in operations, risk profile, or regulatory environment warrant additional testing. Such drills shall be designed to assess the practical readiness of alternate facilities, recovery procedures, communication protocols, personnel accountability, technological failover capacity, and command-and-control arrangements under realistic disruption scenarios. Each exercise shall be documented in detail, including the scenario tested, participants involved, observed deficiencies, response times, decision points, and the degree to which essential functions were maintained or restored. Following each drill, the organization shall complete a **corrective action review** identifying required improvements, responsible personnel, implementation deadlines, and verification methods to confirm remediation. No deficiency shall be treated as insignificant if it reveals a gap in the organization’s capacity to protect clients, preserve operations, or comply with applicable obligations during an emergency. Lessons learned shall be formally incorporated into revised continuity plans, training materials, and operational

procedures. **Testing without correction is performance without substance; therefore, every identified weakness shall be addressed with measurable and timely remedial action.**

Where appropriate, ASYLUM RESEARCH & GLOBAL ASSISTANCE shall integrate business continuity planning with its broader obligations concerning confidentiality, data security, client care, regulatory compliance, and institutional governance, ensuring that continuity measures do not merely preserve operations in form, but preserve them in a manner consistent with **professional duty, legal integrity, and unwavering organizational accountability**.

V. CRISIS MANAGEMENT

ASYLUM RESEARCH & GLOBAL ASSISTANCE shall maintain a formal, disciplined, and immediately actionable crisis management framework designed to preserve life, protect sensitive information, secure operational continuity, and ensure lawful, accurate, and ethically uncompromising decision-making under conditions of acute disruption. Crisis management shall be treated as a governance function of the highest priority, requiring prompt escalation, centralized command, verified information flow, and documented accountability at every stage. No response shall be improvised where structured authority, clear reporting lines, and legally defensible procedures are required.

1. Crisis Response Team

The **Crisis Response Team** shall be composed, at a minimum, of the Chief Executive Officer, Chief Financial Officer, General Counsel, and Communications Director. This composition reflects the organization's need to integrate executive authority, financial oversight, legal risk assessment, and strategic messaging into a single decision-making structure capable of acting with speed, precision, and integrity. The Chief Executive Officer shall serve as the primary executive authority and final internal decision-maker unless immediate operational necessity requires temporary delegation. The Chief Financial Officer shall assess financial exposure, insurance notification obligations, liquidity implications, vendor dependencies, payroll continuity, and any emergency funding requirements. The General Counsel shall provide authoritative direction on legal privilege, preservation of evidence, regulatory reporting, contractual obligations, employment matters, civil liability, confidentiality, and any mandatory notifications to authorities or counterparties. The Communications Director shall manage internal and external communications, ensuring that all statements are accurate, coordinated, consistent, and legally cleared before release.

The Crisis Response Team shall have the authority to convene immediately upon activation, either in person or through secure remote means, and shall remain operational until the crisis has been stabilized and transitioned into recovery management. Each member shall be responsible for maintaining current contact information, alternate communication channels, and access to relevant emergency documentation, including continuity plans, legal hold procedures, insurance policy records, vendor escalation lists, and internal reporting templates. The team shall act in accordance with the principles of **lawful necessity, operational discipline, confidentiality, and documented accountability**.

2. Triggers for Activation

Activation of the Crisis Response Team shall occur immediately upon the existence or reasonable anticipation of any event that materially threatens personnel safety, organizational continuity, legal compliance, financial stability, data integrity, reputation, or the ability to perform essential functions. The principal triggers include, without limitation, a **major security incident**, the death or incapacity of a key person, discovery of fraud, and a natural disaster. For purposes of this policy, a major security incident includes any incident involving violence, credible threat, unauthorized access, significant breach of physical or digital security, hostage or coercive event, or any condition that reasonably creates a substantial risk to life, liberty, property, or confidential information.

The death, serious illness, incapacitation, disappearance, or legal unavailability of a key person shall constitute an activation trigger where such person's role is material to governance, operations, finance, legal compliance, communications, or mission-critical decision-making. Discovery of fraud shall include any credible indication of misappropriation, falsification, embezzlement, bribery, unauthorized transactions, forged records, concealment of assets, or intentional misrepresentation affecting internal controls, donor confidence, regulatory standing, or contractual integrity. A natural disaster shall include any event, whether declared or undeclared by public authorities, that materially impairs facilities, personnel access, communications, supply chains, information systems, or the continuity of essential functions, including but not limited to flood, earthquake, fire, severe storm, tornado, epidemic conditions, or widespread infrastructure failure.

Activation decisions shall be made on the basis of credible information, not speculation, but **reasonable suspicion and material risk are sufficient to warrant escalation**. Where uncertainty exists, the default presumption shall favor activation if delay could reasonably increase harm, diminish evidentiary integrity, compromise safety, or impair the organization's ability to meet legal or ethical obligations. The organization shall not wait for full confirmation where immediate action is necessary to prevent escalation or preserve evidence.

3. Incident Command Structure, Communication Protocols, and Media Response Guidance

Upon activation, the organization shall operate under a defined **incident command structure** designed to eliminate ambiguity, prevent conflicting instructions, and ensure that all operational activity is directed through a single coordinated chain of authority. The Crisis Response Team shall designate a lead incident coordinator, who may be the Chief Executive Officer or another appropriately authorized executive, and all functional responses shall be aligned to that coordinator's directives. Operational functions shall be assigned according to competency and urgency, with the General Counsel overseeing legal and evidentiary safeguards, the Communications Director controlling messaging, the Chief Financial Officer managing financial controls and emergency expenditure authorization, and other relevant personnel engaged only as necessary and under instruction. No employee, consultant, contractor, or representative shall issue instructions outside their delegated authority or communicate unapproved information to external parties.

All communication during a crisis shall be governed by the principles of **need-to-know access, factual accuracy, secure transmission, and message consistency**. Internal communications shall be limited to persons who require the information to perform assigned duties. Sensitive information shall be communicated only through approved secure channels, and all material updates shall be recorded in a contemporaneous incident log. Employees shall be instructed to preserve evidence, avoid speculative commentary, and refrain from deleting, altering, or disclosing potentially relevant materials. Where legal hold is required, it shall be issued immediately and shall supersede ordinary retention or disposal practices. The organization shall maintain a strict prohibition against informal or contradictory statements that could compromise legal position, safety, or public confidence.

External and media communications shall be centralized exclusively through the Communications Director, subject to legal review by the General Counsel and final approval by the designated executive authority. No employee or representative shall provide off-the-record commentary, speculate on cause or responsibility, confirm unverified facts, or respond to media inquiries unless expressly authorized. Public statements shall be limited to verified information necessary to protect safety, maintain trust, comply with law, and avoid material misinformation. Communications shall be measured, factual, and non-inflammatory, and shall never minimize harm, obscure accountability, or imply certainty where facts remain under investigation. The organization shall ensure that all public-facing language is **accurate, disciplined, and ethically irreproachable**, with particular attention to confidentiality, victim protection, legal exposure, and the preservation of investigative integrity.

Where an incident involves law enforcement, emergency responders, insurers, regulators, landlords, insurers, technology providers, financial institutions, or other third parties, all engagement shall be coordinated through the Crisis Response Team to avoid duplication, inconsistency, or waiver of rights. Any external notification required by contract, regulation, or law shall be made promptly and in the prescribed manner. The organization shall document the time, content, recipient, and legal basis of each material communication.

4. Post-Incident Review

A formal **post-incident review** shall be completed no later than thirty (30) days after the incident has been stabilized, unless extraordinary circumstances require a limited extension approved by the Chief Executive Officer and General Counsel. The review shall be comprehensive, candid, and evidence-based. Its purpose shall not be symbolic or perfunctory, but corrective, preventive, and institutionally instructive. The review shall assess the chronology of events, the adequacy of activation decisions, the effectiveness of command and communication protocols, the sufficiency of resources, the accuracy and timeliness of notifications, the appropriateness of media handling, the preservation of evidence, and the legal, financial, operational, and human impacts of the incident.

The organization shall document **lessons learned** in a formal written record that identifies root causes, control failures, missed escalation points, successful interventions, and required policy or procedural amendments. Where deficiencies are identified, corrective action shall be assigned to named responsible persons with deadlines for completion and follow-up verification. The

organization shall not permit lessons learned to remain aspirational; they shall be translated into measurable reforms, training updates, control enhancements, and where appropriate, disciplinary or contractual action. In cases involving fraud, serious misconduct, security breach, or material negligence, the review shall include consideration of internal accountability measures, referral to competent authorities, and strengthening of governance controls to prevent recurrence.

All review materials, findings, and corrective actions shall be retained as confidential internal records subject to legal privilege where applicable. The organization shall treat the post-incident review as an essential component of institutional integrity, recognizing that a crisis is not adequately managed unless the organization emerges with **clearer controls, stronger accountability, and demonstrably improved resilience**.

Signed by:

Sergei Khrabrykh

President, Asylum Research & Global Assistance

Date: 18 January 2024