

Risks & Controls: Areas of Internal Controls; Donor Due Diligence Checklist & Readiness Roadmap

Structure of session

1. **Risks & Controls.** Understanding the risk-control tangle.
2. **Internal Controls.** Internal control areas that donors examine closely.
3. **Due Diligence Checklist & Readiness Roadmap.** Completing the full circle from Session 1.

Two Pillars of Pre-Grant Due Diligence

Institutional Due Diligence

Is the organisation legitimate, well governed, and capable of delivering the programme?

- Constitutional: legal registration & regulatory compliance
- Statutory registrations & regulatory compliance
- Governance
- Mission fit
- Policies & procedures
- Programmatic track record & M&E systems
- Visibility

- Past donor relationships and references

Financial Due Diligence

Can the organisation be trusted to receive, manage and report on donor funds accurately?

- Annual financial statements: state of financial health & progress
- Audit and assurance
- Internal financial controls
- Budgeting
- Grant management
- Banking arrangements
- Accounting systems
- Procurement
- HR

Part 1: Risks & Controls

Why Understand Risk & Risk Management

- Risk is now a must-discuss in the NGO-funder relationship. The idea is how to understand, capture and manage risks
- Robust risk management is (a) basic to an effective organisation and (b) ensures better delivery of services to the community
- Fundamental concepts: **Risk Appetite** (willingness to take risk to achieve objectives) and **Risk Tolerance** (ability/boundary to take risk, i.e. acceptable deviation from risk appetite). Risk appetite is about "taking risk"; risk tolerance is about "controlling risk." Risk appetite denotes risk profile at an aggregate level; risk tolerance applies at activity level, case by case
- Risk management is how to bridge the gap between risk appetite and risk tolerance
- Understand need for internal controls commensurate with risks being mitigated

Why Risk Management Is Important for NGOs

1. Financial stability
2. Operational efficiency
3. Compliance management
4. Disciplined planning
5. Informed decision making
6. Reputation management
7. Building trust
8. Improved communication
9. Long-term impact & sustainability

Risk: Key Concepts

- **Threat:** A danger in the environment, a potential cause of harm, e.g. legislative changes, technology, competition, inflation, globalisation, etc.
- **Risk:** The probability and potential impact on achievement of objectives while encountering a threat.
- **Internal & external risks:** Internal risks: personnel issues, technology issues, etc. within the organisation. External risks: economic, political, legal, act of God, etc. in the external environment.

Residual risk: *the risk which inevitably remains after all reasonable mitigation measures have been taken. No organisation is completely free from risk; the environment will always contain risk.*

Types of Risks Facing Organisations

- **Ethical:** Due to unethical behaviour
- **Operational:** Inability to achieve objectives; capacity/competence gaps; funding & access constraints
- **Financial:** Improper financial planning and management
- **Reputational:** Damage to image and reputation

- **Safety:** Accident / illness
- **Security:** Violence / crime
- **Fiduciary:** Breach of trust: corruption, fraud, theft, diversion
- **Legal / compliance:** Violation of / non-compliance with laws or regulations
- **Information:** Data breach/loss, digital risk, systems breach
- **Competition:** Competitors for service delivery

Risk: Key Concepts (Continued)

Risk Management / Mitigation

- Organisational practices, policies & procedures (P&Ps) that reduce the probability of risks being realised and limit harmful consequences

Enterprise (Integrated) Risk Management (ERM)

- Risk management that considers, combines and prioritises assessed risks in all risk areas (security, fiduciary, operational, informational and reputational) to strategise and implement mitigation measures

“Risk mitigation is risk reduction. It cannot be made zero.”

Risk Management Policy: Need

- Donor audits for ongoing grants/due diligence by prospective donors
- Need to instil a sense of identifying, understanding and addressing risks in the organisation as it grows; basic to a for-profit entity
- Create awareness about risk-mitigation strategies when faced with risks in respective areas of work
- Staff embrace and own the risk-management process
- Is a tool for governance and control

Risk Management Process

- Risk universe analysis
- Risk identification
- Risk assessment: risk assessment matrix based on likelihood and impact of identified risks

Risk assessment matrix (Likelihood vs Consequence)

Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain (5)	Low	Medium	High	High	High
Likely (4)	Low	Low	Medium	High	High
Possible (3)	Low	Low	Medium	Medium	High
Unlikely (2)	Low	Low	Low	Low	Medium
Remote (1)	Low	Low	Low	Low	Low

After assessment:

1. **Prioritise risks:** Risks to be taken up for mitigation
2. **Risk response:** Risk registers with roles and responsibilities of staff
3. **Monitoring**
4. **Reporting**

Internal Controls

Business practices that serve as "checks and balances" on internal stakeholders (staff/key functionaries) and/or external stakeholders (vendors) to reduce risk. To the donors, they assure that funds will be effectively utilised for the intended purpose.

Rationale for Internal Controls

- Compliance: with laws and regulations
- Accountability: promote accountability
- Fraud prevention: preventing fraud and embezzlement
- Operational efficiency: improving accuracy and timeliness of program and financial delivery and reporting

Internal Controls: Types

- Preventive: approvals, authorisations, verifications, reconciliations, reviews of operating performance
- Detective: audits and reviews, account reconciliations, physical inventories
- Corrective: remedy problems through detective controls
- Physical controls: security measures like locks, alarms etc.

Donor Due Diligence & Internal Controls

A direct correlation: every due diligence lens maps to a core internal control component.

Donor due diligence focus	Internal control component
Financial Management Assessment: Reviewing budgets, accounting systems, and audit history before an award	Control Environment: Tone at the top, ethics policies, lines of authority
Governance & Compliance Review: Checking board oversight, policies, and legal registration	Risk Assessment: Identifying and prioritizing risks to funds and mission delivery
Risk & Fraud Screening: Background checks, sanctions screening, and fraud-risk indicators	Control Activities & Information Systems: Segregation of duties, approvals, reconciliations, and reporting systems
Program & Results Monitoring: Verifying that funded activities deliver intended outcomes	Monitoring Activities: Ongoing supervision, internal audit, and corrective follow-up

A Reinforcing Cycle

Strong internal controls and favorable due diligence results reinforce each other continuously.

1. **Strong Internal Controls:** Clear policies, segregation of duties, active oversight
2. **Favorable Due Diligence:** Fewer findings, faster review, higher confidence rating
3. **Funding Secured:** Grants awarded or renewed, fewer restrictive conditions
4. **Reinvestment in Controls:** Funding builds systems, staff, and audit capacity, which leads back to strong internal controls

When Controls Are Weak

- Delayed disbursements while donors verify systems
- Restricted funding and added reporting conditions
- Reputational damage among peer donors and partners
- Loss of eligibility for future grants

Part 2: Internal Controls

Key Areas of Internal Controls in NGOs

Internal controls can be grouped into one of the following buckets: (a) Financial (b) Operational (c) Compliance. Illustrative but not exhaustive; discussed in the following sections.

1. Legal & Compliance (done in institutional DD)
2. Governance
3. Budget
4. Purchase / Procurement
5. Human Resource Management
6. Assets / Inventory Management
7. Accounting
8. Cash and Bank
9. Donor Reporting
10. Proceedings & Penalties
11. MIS & Software

Governance & Delegation

- Current general and governing body members: due process of appointment, change or rotation as per rules with proper documentation as per rules. Too long a holding of positions is a negative
- Founder as Chief Functionary for a long duration is evaluated against strategic contribution for such periods
- Key office bearers (Chairman, Secretary and Treasurer): their association and discharging of roles and responsibilities

- Blood relative/conflict of interest is a negative; independence of Board is questionable
- Related person (ITA 2025; Specified person, Section 13 ITA 1961): transactions and benefits thereof
- Any beneficial relations with other organisations
- Governing body members duly updated with registering authority, Darpan and FCRA
- Number and periodicity of meetings of general body and governing body as per constitution documents or law
- Attendance and minutes of meetings maintained in minutes register, held with CEO
- Meetings take up items of business as per roles/duties of the respective body laid down in the constitution document
- Formal documentation of action taken on decisions in previous meetings
- Sub-committees delegated Board responsibility should be as per constitution documents, and recommendations be duly approved by the governing body. Sub-committees could normally be FAC, HR, Grantee selection, etc.
- Demonstration of strategic guidance, compliance and internal controls through policies and procedures
- Does the governing board/executive committee have public servants?
- Does the organisation or any directors/trustees have political or faith based affiliations?
- Do key functionaries have a track record of adverse proceedings?
- Does the organisation's work fall within the definition of political nature/party politics?
- Key staff succession risk assessment?
- Does the organisation understand boundaries in matters relating to Advocacy, Rights & Entitlements, Activism, etc.?

Accounts & Finance

Systems & Records

- Fund-based accounting
- Finance policy and systems implemented in letter and spirit
- Accounting software, COA, basis of accounting etc.
- Accounting records: vouchers, supporting bills/invoices for expenses, PO/contract, approvals, printouts, filing
- Monthly and annual closing of books

- Delegation matrix for approvals
- Segregation of duties / checks and balances

Compliance & Assurance

- Maintenance of books of accounts and other records as per Income Tax Act
- Qualification and vintage of accounts/finance staff
- Separate accounting for local, FC and business-incidental
- Data security, backup and audit trail; rectification entries in succeeding period
- Concurrent and internal audit
- HO-branch accounting and reconciliation

Record Keeping

Rule 187 of ITR 2026: Specified Books of Accounts

- Cash book
- Ledger
- Journal
- Copies of bills issued
- Original bills received and payments made

Other Documents

- Record of all projects and institutions run by the organisation
- Record of income of the organisation during the tax year
- Record of application out of the income during the tax year
- Record of specified application out of income of preceding years
- Record of voluntary contribution with a specific direction to form corpus
- Record of contribution received under 80G(2)(b), treated as corpus
- Record of loans and borrowings
- Record of properties held by the assessee
- Record of related persons as per Section 355 of ITA 2025
- Any other document

Since August 2022, Rule 17AA of the Income Tax Department specifies what records to maintain, in what form, where, and for what period, and the consequences for non-compliance.

Form, Place & Period

- Form: written, electronic or digital form, print-outs, or any other electromagnetic data storage device
- Place: kept at the "registered office"; if not, intimate the Assessing Officer in writing with a Board Resolution within 7 days with full addresses of other places
- Period: kept and maintained for six years from the end of the relevant tax year

Donors may stipulate record-retention clauses in their respective grant contracts. For other records, specific provision may be made in policy.

Costs, Budgets and Budgetary Control

- Understanding the concept of costs: functional and natural heads
- Policy framework for allocation of costs: HR, travel, utilities mainly
- Common cost and apportionment as per common-cost policy
- Budget formulation and approval process: annual master budget including all projects
- Templates may vary by donor but the basic principles of formulation are the same: LOE, unit of measurement and unit cost for an activity, budget by line item and total budget
- Expenditure reporting vis-à-vis budget: rolled up or detailed
- Budget monitoring process: budget vs actual, derived from software
- Budgetary control process: action based on tolerance/variance permitted, which may vary by donor

Human Resources

- Org structure: updated
- Recruitment, selection, engagement contract
- Employee vs consultant vs contractual dilemma
- Compensation and breakup: compliance with social security laws
- Employee benefits: leave, insurance coverage, gratuity
- Payroll and allocation of employee costs

- Attendance records and allocation to donor projects
- Performance appraisal
- Disciplinary action
- Employee strength currently, including in finance function
- Understanding of various social security laws (central and state) so policy and procedures are as per law

HR recalibration in all matters requiring compliance with the New Labour Codes. Team due diligence: leadership, experience, alignment with mission, vision and culture values, transparency, etc.

Procurement

Procurement Policy

- Most activities in grants fall within realm of procurement
- Sample procurement transactions insisted upon by donors to validate policy implementation
- Team's understanding and compliance of Procurement Policy for goods, services and works
- Does the donor insist on following its own procurement policy/guidelines?
- Dedicated admin staff to handle procurement in the organisation
- Conflict of interest, ethics and transparency issues

Fixed Assets & Inventory

- Distinction between asset and inventory understood by staff
- Acquiring asset and inventory following procurement process laid down in policy
- Recording, marking, issue and return, upkeep, depreciation, verification, loss, sale due to obsolescence of fixed assets
- Recording, issue and return, verification, disposal of inventory not needed/useful
- Insurance of assets to cover loss due to various reasons
- Recording of land and building in books

- Fixed assets presented separately in FC audited financials and annual reporting for FC assets in FC-4

Cash & Bank

Petty Cash & Banking

- Petty cash: custody, administration and replenishment. Restrict petty cash to small office payments
- Reduce cash handling and transactions to the bare minimum since banking is universal; good practice
- Provisions on banking in constitution document: sometimes only a nationalised bank / SB account is insisted upon
- Local and FCRA accounts: do's and don'ts
- Dedicated bank account for grants
- Recording and treatment of interest in pool account

Controls & Reconciliation

- Signatory to bank accounts (see constitution documents): dual signatories, non-related, prefer net banking
- Bearer payments: Section 40A(3) provisions
- Bank reconciliation and follow-up
- Minimise visits to branch; sometimes one person engaged for banks only
- Bank statement copies for past 2 years to ascertain operations are through banking channels

Donor Grants

- Current status of grant funding: donor funding is a factor of annual budgets and spends for past few years
- Besides audited (historical) data, donors obtain projections of grants and income in future years
- Understanding the donor is essential for positioning your organisation

- Understanding and internal dissemination of the grant contract
- Grant compliance checklist: accounting, utilisation and reporting differ by donor: FC, CSR, others
- Cost center accounting for ensuring fund based accounting
- Programme & financial reporting: template, periodicity, etc. for each grant contract
- Timely request for course correction and revision
- Community contribution, leverage, cost matching help build your case
- Communication is key

Compliance: Proceedings and Penalties

- Income Tax: assessments, proceedings
- TDS/TCS deposit, return related
- FCRA: violations and offences
- Labour Codes: PF, ESI, PT, gratuity, LIN, Annual Return
- GST related
- Proceedings against Chief Functionary/Board members

MIS & Software

1. Accounting, TDS, Assets
2. HR: payroll, timesheet, leave, etc.
3. Audit
4. Programme MIS
5. Grant Management for donor entities
6. Integrated MIS (all parts on the same application)

Part 3: Due Diligence Checklist & Readiness Roadmap

Sample of Donor Due Diligence Checklist

Revision #1

Created 2026-10-14 06:21:20 UTC by Pooja

Updated 2026-10-14 06:25:18 UTC by Pooja