국제투명성기구 한국본부
한국투명성기구
TRANSPARENCY INTERNATIONAL-KOREA

Risk Management Procedure for TI-Korea Chapter

Table of Contents

1. Introduction
2. Risk Identification
3. Risk Analysis
4. Risk Evaluation
5. Risk Mitigation and Control
6. Monitoring and Review
7. Communication and Reporting
8. Documentation and Record Keeping
9. Continuous Improvement
10. Conclusion

1. Introduction

2. Risk Identification

Risk identification is the foundational step in the risk management process. It involves spotting potential threats or challenges that could impact on the achievement of the organization's objectives. These risks can be internal or external in nature, tangible or intangible, and can vary in terms of probability and potential impact.

2.1. Sources of Risks

Operational Risks: Stemming from the organization's day-to-day activities. Examples could include inefficiencies, human error, system breakdowns, or lack of resources.

- Strategic Risks: Related to the organization's strategic decisions, mission, and vision. For example, choosing to work on a project that might not align with the organization's core values.
- Financial Risks: Related to financial operations and market dynamics. Currency fluctuations, budget overruns, or decreased funding can all pose risks.
- Reputational Risks: Risks that might tarnish the organization's public image or stakeholder trust. This could stem from a scandal, an unhappy stakeholder, or negative media coverage.

2.2. Internal Assessment

Self-Evaluation: Departments within TI-Korea Chapter should conduct a periodic self-assessment to identify vulnerabilities, inefficiencies, or any other operational risks.

- Employee Feedback: Employees can provide crucial insights into day-to-day operational risks and suggest areas of improvement. A confidential feedback mechanism can be beneficial.
- Financial Analysis: Detailed examination of the organization's financial statements and budgetary practices to spot potential financial risks early on.

2.3. External Assessment

Socio-Political Monitoring: With the dynamic socio-political landscape of Korea, it's essential to keep an eye on changes in laws, policies, or public sentiment that might impact the organization.

- Technological Trends: The rapid pace of technological advancements could introduce risks or opportunities. Monitoring these trends ensures that TI-Korea Chapter isn't left behind or vulnerable to emerging tech-related threats.
- Stakeholder Feedback: Regular communication with donors, partners, volunteers, and beneficiaries can provide valuable insights into potential external risks. Surveys, feedback forms, or regular meetings can be instrumental.
- Environmental Scanning: Review of media, academic literature, and reports related to corruption, transparency, and the NGO sector in Korea. This will help in understanding the broader environment and spotting emerging risks.

2.4. Risk Documentation

All identified risks should be documented meticulously in the risk register. This document should include details of the risk, its source, potential impact, likelihood, and any immediate actions taken. Regularly updating this document ensures that all stakeholders have a clear and up-to-date view of the organization's risk landscape.

By investing time and resources in thorough risk identification, TI-Korea Chapter lays the groundwork for the subsequent steps of the risk management process, ensuring that all potential challenges are addressed proactively.

3. Risk Analysis

Risk analysis delves deeper into the identified risks, studying them to understand their nature, potential consequences, and likelihood of occurrence. It enables organizations like TI-Korea Chapter to allocate resources more effectively and prioritize risks based on their significance.

3.1. Objective and Purpose

Understanding the risks is pivotal to making informed decisions.
Risk analysis:

- Provides a detailed understanding of each risk.
- Determines the inherent risk level before any controls or mitigation measures.
- Enables prioritization based on impact and probability.

3.2. Qualitative Analysis

A subjective assessment that classifies risks based on their severity and likelihood without assigning specific numerical values.

- Descriptive Scales: Risks can be categorized as 'Low', 'Medium', or 'High' based on their perceived impact and likelihood.
- SWOT Analysis: Strengths, Weaknesses, Opportunities, and Threats can be used to gain insights into internal and external risks.

- Brainstorming & Expert Opinion: Engaging team members and experts in the field to discuss and provide insights on risks.

3.3. Quantitative Analysis

A more numerical and data-driven approach to understand the potential impact of risks.

- Historical Data: Analyzing past incidents and their consequences to predict potential future outcomes.
- Statistical Models: Use of statistical tools and techniques to assess the potential magnitude and frequency of risks.
- Sensitivity Analysis: Understanding how changes in various factors can impact on a particular risk. For example, how changes in funding might affect project completion.

3.4. Risk Scoring & Ranking

After understanding both the qualitative and quantitative aspects:

- Risk Matrix: A common tool where risks are plotted based on their likelihood on one axis and their impact on another. This visual representation helps in quick prioritization.
- Risk Score: Assigning numerical values based on the combined assessment of impact and likelihood. For instance, a risk with a medium likelihood (value 2 on a scale of 1-3) and high impact (value 3 on a scale of 1-3) would have a risk score of 6.

3.5. Dependencies and Aggregation

Understanding how risks interrelate.

- Risk Dependencies: Some risks might be contingent on others. For instance, a reputational risk might emerge as a consequence of a financial risk.
- Aggregated Impact: Recognizing that the collective impact of multiple risks occurring together might be different from them happening independently.

3.6. Assumptions and Limitations

Every analysis will have its assumptions and limitations.
It's essential to:

- Document assumptions made during the analysis.
- Understand limitations, like the lack of historical data or changing external factors, which might influence the accuracy of the analysis.

By thoroughly analyzing risks, TI-Korea Chapter can make well-informed decisions, ensuring that resources are efficiently allocated and the most significant risks are addressed with priority.

4. Risk Evaluation

Risk evaluation is a decisive step in the risk management process where the organization determines the significance of the analyzed risks and decides on the appropriate next steps. It involves comparing the results of the risk analysis against pre-established criteria to determine if the risk is acceptable or if it requires further attention.

4.1. Objective and Purpose

Risk evaluation:

- Helps prioritize resources and interventions.
- Determines which risks can be accepted and which require mitigation.
- Assures stakeholders that risks are being managed systematically and diligently.

4.2. Criteria Establishment

Before evaluating risks, it's imperative to establish clear criteria:

- Thresholds: Define the boundaries for risk acceptance. For instance, any risk with a score above 'X' is deemed unacceptable and requires action.
- Organizational Appetite: Understand the level of risk TI-Korea Chapter is willing to accept in pursuit of its objectives.

4.3. Risk Comparison

After the analysis phase:

- Benchmarking: Compare the identified risks against the pre-established criteria.
- Prioritization: Based on the risk scores and organizational thresholds, determine which risks need immediate attention.

4.4. Decision on Risks

For every identified risk:

- Accept: If a risk is within the acceptable thresholds and aligns with the organization's risk appetite, it may be accepted without further action.
- Transfer or Share: Risks might be transferred (for instance, through insurance) or shared with partners if doing so aligns with strategic objectives.
- Avoid: Some risks might be so detrimental that the best course of action is to avoid them altogether, even if this means stopping a project or changing strategies.
- Mitigate: If risks are above the acceptable level but can't be avoided, plans to reduce their impact or likelihood are made.

4.5. Residual Risk Assessment

Even after mitigation efforts, there might be some remaining risk (residual risk).

It's essential to:
Evaluate the level of this residual risk.
Decide if it's within the acceptable boundaries or if further mitigation is required.

4.6. Cost-Benefit Analysis

Sometimes, the cost of mitigating a risk might outweigh its potential impact. In such cases:

- Assess the costs associated with mitigation strategies.
- Compare them against the potential benefits or losses prevented.

- Make decisions that ensure the organization's resources are utilized optimally.

4.7. Stakeholder Input

Risks might affect various stakeholders differently:

- Engage relevant stakeholders to get their perspective on risk acceptance.
- Ensure that decisions align with both organizational objectives and stakeholder expectations.

4.8. Documentation

All decisions and justifications during the risk evaluation phase should be meticulously documented. This ensures:

- Transparency in the decision-making process.
- A reference point for future evaluations or audits.

By concluding the risk evaluation process, TI-Korea Chapter ensures that identified risks are addressed based on their significance and the organization's capacity and appetite for risk. It lays the groundwork for the next steps, primarily risk mitigation and monitoring.

5. Risk Mitigation and Control

Risk mitigation is about putting strategies and measures in place to reduce the negative effects of threats and vulnerabilities. This involves either reducing the likelihood of the event happening, minimizing the impact if it does occur, or setting up mechanisms to cope with the consequences.

5.1. Objective and Purpose

Risk mitigation:

- Aims to lessen the potential adverse effects of risks.
- Ensures that risks remain within acceptable boundaries.
- Demonstrates proactiveness in managing threats and vulnerabilities.

5.2. Risk Avoidance

This strategy involves making decisions to circumvent risk altogether.

- Project Termination: If a project presents inordinate risks, consider termination or redesign.
- Strategy Redefinition: Alter strategies that might lead to high levels of unacceptable risks.

5.3. Risk Reduction

Taking steps to minimize the impact or likelihood of the risk.

- Training: Equip staff with skills to handle potential risks, e.g., ethical training to reduce corruption-related risks.
- Process Enhancement: Refining operations to minimize chances of errors or inefficiencies.

5.4. Risk Transfer

Sometimes, it’s more viable to transfer the risk elsewhere.

- Insurance: Obtain coverage to protect against potential financial losses.
- Partnerships: Collaborate with partners who might be better equipped to handle certain risks.

5.5. Risk Acceptance

Recognizing the risk but deciding against active mitigation due to various reasons.

- Contingency Plans: Even if the risk is accepted, have a plan in place to handle potential consequences.
- Resource Allocation: Set aside resources (time, funds, etc.) in anticipation of potential risk realization.

5.6. Risk Financing

Allocating funds to handle the consequences of risks.

- Reserve Funds: Establish an emergency fund for unpredictable threats.
- Budgeting: Allocate budget lines for specific risk management activities.

5.7. Policy Actions for TI-Korea

Given TI-Korea's focus on corruption and integrity, the following policy actions should be considered:

1. Ethical Guidelines: Develop strict ethical guidelines and ensure that all staff, volunteers, and associates understand and comply. Regular training and reinforcement are crucial.

2. Whistleblower Policy: Establish a secure and anonymous whistleblower policy where individuals can report suspicions or instances of corruption without fear of reprisal.

3. Collaboration with Authorities: Work in tandem with local regulatory and legal entities to ensure that any corruption-related incidents are addressed legally and justly.

4. Public Reporting: Maintain transparency by publicly disclosing financial statements, project outcomes, and any incidents of integrity breach. This not only fosters trust but also sets a benchmark for other organizations.

5. Stakeholder Engagement: Regularly engage with donors, beneficiaries, and other stakeholders to understand their concerns, expectations, and get feedback on TI-Korea's initiatives.

6. Regular Audits: Conduct regular internal and external audits to ensure compliance with all established rules, regulations, and ethical guidelines.

7. Community Outreach: Develop programs to educate the community about the adverse effects of corruption, and how they can play a part in mitigating it.

5.8. Continuous Monitoring and Refinement

- Feedback Loops: Set up mechanisms to gather feedback on mitigation strategies to understand their effectiveness.
- Periodic Reviews: Every strategy should be reviewed periodically to ensure its relevance and effectiveness in the current risk landscape.
- By concluding the risk mitigation phase, TI-Korea Chapter ensures that risks are not just identified and analyzed but also acted upon. It's an affirmation of the organization's commitment to its mission and stakeholders.

6. Risk Monitoring and Review

Monitoring and review are pivotal in ensuring the continuous effectiveness of the risk management process. It involves regularly tracking and evaluating the risks and the mitigation strategies in place. Adjustments are made based on lessons learned, changes in the risk environment, and feedback from stakeholders.

6.1. Objective and Purpose

Risk monitoring and review:

- Validates the effectiveness of the risk management process.
- Ensures that the organization adapts to changes in its risk profile.
- Reinforces accountability and transparency in handling risks.

6.2. Key Performance Indicators (KPIs)

Establish clear metrics to gauge the effectiveness of risk management efforts.

- Risk Reduction: Measure the number or severity of risks reduced over a period.
- Incident Response Time: Track the speed at which risk-related incidents are addressed.
- Stakeholder Feedback: Monitor feedback scores or satisfaction levels related to risk management efforts.

6.3. Risk Re-assessment

Regularly revisit and assess risks to understand any changes in their nature, impact, or likelihood.

- Trending Risks: Identify risks that might be increasing in terms of their potential impact or likelihood.
- Newly Emerged Risks: Regular scanning for new risks that weren't identified in previous assessments.

6.4. Review of Mitigation Strategies

Effectiveness Review: Evaluate the strategies to determine if they are yielding the desired results in risk reduction.

- Cost Analysis: Assess the cost-effectiveness of the risk mitigation efforts.

6.5. Stakeholder Feedback Loop

- Regular Consultations: Engage with internal and external stakeholders to get their insights and feedback on risk management practices.

- Feedback Integration: Incorporate valuable stakeholder feedback into the risk management process.

6.6. Documentation and Reporting

- Risk Management Dashboard: Develop a real-time dashboard showcasing the status of various risks, their mitigation statuses, and any incidents.
- Periodic Reports: Regularly update stakeholders, especially senior management and the board, about the status of risk management efforts.
- Incident Logs: Maintain detailed logs of any risk-related incidents, the responses taken, and lessons learned.

6.7. Continuous Improvement

- Lessons Learned: After every major risk-related incident or at regular intervals, gather the team to discuss what went well and what could have been done better.
- Training and Development: Based on monitoring and review findings, identify areas where the team may need further training or resources.
- Tool and Technology Review: Periodically assess if the tools and technologies used for risk management are still fit for purpose or if better alternatives are available.

6.8. External Audits

Engage external experts to conduct audits of the risk management practices. This:

- Offers an unbiased perspective on the effectiveness of the risk management process.
- Helps identify areas of improvement that might have been overlooked internally.

By continually monitoring and reviewing risks, TI-Korea Chapter ensures that its risk management process is dynamic, adaptive, and continuously aligned with its objectives and the expectations of its stakeholders.

7. Communication and Consultation

Effective communication and consultation form the backbone of successful risk management. Ensuring that all relevant parties, both internal and external, are well-informed and actively involved in the risk management process is critical for its efficiency and credibility.

7.1. Objective and Purpose

Communication and consultation aim to:

- Foster a collaborative environment where risks are transparently shared and collectively addressed.
- Enhance stakeholder trust through openness and clarity.
- Harness diverse perspectives and expertise in risk management.

7.2. Internal Communication

Ensuring that team members, departments, and internal stakeholders are aligned.

- Regular Updates: Schedule regular risk management updates, discussions, and brainstorming sessions.
- Training Sessions: Equip staff with the skills and knowledge needed to identify, assess, and mitigate risks.
- Feedback Channels: Establish clear channels for employees to voice their concerns, offer insights, or report potential risks.

7.3. External Communication

Engaging with external stakeholders like partners, donors, beneficiaries, and the general public.

- Stakeholder Briefings: Organize periodic briefings or updates on the organization's risk management status and actions.
- Public Reports: Publish annual or bi-annual risk management reports, detailing achievements, challenges, and future plans.
- Collaborative Workshops: Host workshops with partners or industry peers to discuss shared risks and potential collaborative mitigation strategies.

7.4. Consultation Mechanisms

Effective consultation ensures the risk perspective is broad and comprehensive.

- Focus Groups: Engage specific groups of stakeholders to delve deep into particular risk areas.
- Surveys and Feedback Forms: Gather structured feedback from a wide audience on risk perceptions and management effectiveness.
- Expert Panels: Engage experts in risk management or specific fields to provide guidance and advice.

7.5. Channels of Communication

Determine the most effective ways to communicate with different audiences.

- Digital Platforms: Websites, email newsletters, and social media channels to disseminate information and gather feedback.
- Physical Meetings: In-person meetings, conferences, and seminars to foster direct interaction and collaboration.
- Printed Materials: Brochures, reports, and other printed materials for broader distribution.

7.6. Sensitivity and Confidentiality

Given the nature of some risks, especially those related to integrity and corruption:

- Confidential Channels: Establish secure channels for sensitive communications, such as reporting corrupt practices.
- Data Protection: Ensure that sensitive data, especially concerning stakeholders, is protected and only shared with authorized personnel.

7.7. Feedback Loop

A continuous feedback loop ensures that the communication strategy evolves based on stakeholder needs.

- Feedback Analysis: Regularly analyze feedback to identify areas of improvement in communication strategies.
- Iterative Updates: Periodically update communication plans, tools, and channels based on stakeholder feedback and changing organizational needs.

7.8. Crisis Communication

Plan for scenarios where immediate and clear communication is essential.

- Crisis Communication Plan: Establish a plan detailing how to communicate during and after a risk-related crisis, detailing roles, channels, and messaging.
- Spokesperson Training: Ensure that designated spokespeople are trained to handle media and public inquiries during crises.

By actively communicating and consulting with stakeholders, TI-Korea Chapter ensures that its risk management process is inclusive, transparent, and adapted to the evolving needs of its community.

8. Documentation and Record Keeping

For any organization, especially one addressing sensitive topics like integrity and corruption, maintaining meticulous documentation and records is paramount. It not only serves as evidence of proactive risk management but also ensures accountability, transparency, and traceability.

8.1. Objective and Purpose

Maintaining proper documentation aims to:

- Provide a historical record of decisions, actions, and incidents.
- Ensure compliance with legal and regulatory requirements.
- Enable efficient review and audit of risk management practices.
- Foster trust among stakeholders through transparent record-keeping.

8.2. Types of Documentation

- Risk Registers: Maintain an up-to-date record of identified risks, their assessments, and mitigation strategies.
- Incident Logs: Document any risk-related incidents, the actions taken, outcomes, and lessons learned.
- Policies and Procedures: Maintain updated versions of all risk management policies, procedures, and guidelines.
- Training Records: Document training sessions, participants, content covered, and feedback.

8.3. Storage and Accessibility

- Centralized Database: Use a secure, centralized database or risk management software to store all documentation.

- Access Control: Ensure that only authorized individuals can access sensitive or confidential records. Use roles and permissions to restrict access.
- Backup and Recovery: Implement regular backups and establish a recovery plan in case of data loss.

8.4. Data Protection and Confidentiality

Given the sensitive nature of the work of TI-Korea Chapter:

- Encryption: Use encryption tools to protect sensitive documents, especially those stored digitally.
- Data Retention Policies: Define how long specific documents should be retained and establish a secure disposal procedure for outdated records.
- Confidentiality Agreements: Ensure that staff members and other stakeholders sign confidentiality agreements when accessing sensitive data.

8.5. Regular Audits

- Internal Audits: Conduct periodic internal audits to ensure that documentation is up-to-date, accurate, and in line with organizational policies.
- External Audits: Engage third-party auditors occasionally to validate the documentation process and provide an unbiased evaluation.

8.6. Revision and Updates

- Version Control: Implement version control systems to track changes made to documents over time.
- Review Cycles: Establish a regular review cycle for critical documents to ensure they reflect the current risk landscape and organizational practices.

8.7. Stakeholder Communication

- Transparency Reports: Share non-confidential documentation, like annual risk management reports, with stakeholders to promote transparency.
- Feedback Channels: Provide stakeholders with channels to query, comment on, or provide feedback about the documentation.

8.8. Legal and Regulatory Compliance

- Regulation Mapping: Identify and map out key regulations and laws pertaining to documentation and record-keeping for the sector.
- Compliance Checks: Regularly check that the organization’s documentation practices comply with all applicable regulations.

8.9. Crisis Documentation

- Emergency Protocols: In the event of a crisis, have predefined documentation protocols to ensure that all actions, decisions, and communications are appropriately recorded.

- Lessons Learned: Post-crisis, analyze the documentation to draw out lessons and refine future strategies.

Through diligent documentation and record-keeping, TI-Korea Chapter can demonstrate its commitment to integrity, accountability, and excellence in its risk management endeavors.

9. Continuous Improvement in Risk Management

The landscape of risks is ever-evolving, making continuous improvement not just an aspirational goal but a necessity. For TI-Korea Chapter, as an organization tackling integrity and corruption issues, staying ahead of emerging risks is vital.

9.1. Objective and Purpose

Continuous improvement aims to:

- Adapt and evolve the risk management process in line with changing scenarios.
- Incorporate lessons learned and best practices.
- Ensure the long-term effectiveness and relevance of risk management efforts.

9.2. Review Mechanism

- Annual Reviews: Conduct thorough reviews of the risk management framework, process, and outcomes at least once a year.
- Post-Incident Analysis: After any major risk event or incident, undertake an analysis to determine what went well, what didn't, and how to improve.

9.3. Benchmarks and Comparisons

- Industry Benchmarks: Analyze the risk management practices of similar organizations or industry standards to identify gaps and opportunities for improvement.
- Performance Metrics: Establish and monitor key performance metrics to assess the effectiveness and efficiency of risk management efforts.

9.4. Training and Development

- Regular Training: Provide ongoing training sessions for staff to refresh their knowledge and introduce them to new risk management practices and tools.
- External Courses: Encourage team members to attend external courses, seminars, or workshops on risk management.

9.5. Feedback Mechanism

- Stakeholder Feedback: Actively seek feedback from both internal and external stakeholders on the effectiveness of risk management practices.
- Feedback Integration: Systematically integrate valuable feedback into the risk management process for refinement.

9.6. Technology and Tools Assessment

- Technology Review: Periodically assess the tools and technologies used in risk management for their efficacy, security, and relevance.
- Adoption of New Tools: Stay abreast of advancements in risk management technologies and adopt tools that can enhance efficiency and accuracy.

9.7. Policy and Procedure Updates

- Document Revision: Regularly revise risk management policies and procedures to reflect changes, updates, and improvements.
- Accessibility: Ensure that updated documents are easily accessible to all relevant stakeholders and clearly communicate any significant changes.

9.8. External Audits and Certification

- Third-party Audits: Engage external auditors to evaluate the robustness and compliance of the risk management process.
- Certifications: Aim to achieve certifications in risk management that will not only enhance credibility but also ensure alignment with global best practices.

9.9. Celebrating Successes

- Acknowledgment: Regularly acknowledge and celebrate risk management successes, be it a significant reduction in risks or successful handling of a crisis.
- Reward Mechanism: Introduce a reward mechanism for teams or individuals who excel in risk identification, mitigation, and management.

By emphasizing continuous improvement, TI-Korea Chapter ensures that its risk management practices remain robust, resilient, and aptly equipped to navigate the complexities of the challenges it faces.