Developing a Risk Management Plan

New Partners Initiative Technical Assistance Project (NuPITA)

The New Partners Initiative Technical Assistance (NuPITA) is funded by the United States Agency for International Development (USAID) and implemented by John Snow, Inc. and Initiatives Inc., contract GHS-I-00-07-00002-00.

This report is made possible by the generous support of the American people through USAID. The contents are the responsibility of John Snow, Inc. and do not necessarily reflect the views of USAID or the United States Government.

© 2010 John Snow, Inc.

NuPITA
John Snow, Inc.
44 Farnsworth Street
Boston, MA 02210-1211
Phone: 1.617.482.9485
www.jsi.com

INTRODUCTION

We shall define risk in this context as the possibility that something harmful or undesirable may happen. This could include harm, injury, or abuse to your organization's clients, volunteers, board members, employees, property, or reputation.

Risk management is therefore the procedure that an organization follows to protect itself, its staff, clients, and volunteers. This is an ongoing process.

Remember that it is not possible to eliminate all risk. Your responsibility is to demonstrate that you have recognized the risks you could face and have taken reasonable precautions to prevent them from causing harm to your clients' volunteers, board members, employees, property, or reputation.

This guideline has been developed to help organizations design and implement an effective and proactive risk management plan in response to the circumstances we face in this country because of post-election violence.

This process will help management recognize the risks it is facing, perform risk assessments, and develop strategies to mitigate risks using management resources available to them.

STEPS IN THE RISK MANAGEMENT PROCESS

STEP ONE: Establish your context

Identify, assess, and document potential risks. This involves mapping the following: social scope of risk management (what are your stakeholders facing); the identify and objectives of stakeholders (do you want to ensure minimal financial impact, programmatic impact, etc.); what resources are available to us to help mitigate the effects of the risks; what structures do we have in place to cope with the scenarios that could present themselves.

TIP: *Get a little help. Talk with organizations similar to your own and ask about their experience.*

STEP TWO: Identification of possible risks

Instead of looking at the problem at hand, consider the causes of the problems you might face. The source of the risk should not be ignored but because we face a national problem, we can only effectively address the problems that are presented to us at grantee level.

This means that grantees should look at the threats that they are facing, such as losing money, accidents, casualties, loss of staff, loss of property, etc.

It is helpful to classify the possible risks according to categories, such as: risks to general operations; personnel; program beneficiaries; property, building and equipment; perpetuation.

TIP: *Talk to your stakeholders, find out about their concerns about safety and brainstorm what you might do to address these.*

STEP THREE: Assessment

Once risks have been identified, they must be assessed for potential severity of loss and probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure, in the case of the probability of an unlikely event occurring. This is why, in the assessment process, it is critical to make the best guesses possible in order to properly prioritize.

Table 1: Sample risk matrix for grading risks

	Level of Severity			
		LOW	MEDIUM	HIGH
Likelihood of occurrence	LOW			
	MEDIUM			
	HIGH			

This will help you prioritize the risks as well as allocate resources appropriately.

Table 2:

Description of risk	**Occurrence**	**Severity**	**Rank (prioritization)**	**Status**
Looting of property	Low	Medium	2	New possibility
Loss of staff members	medium	High	1	Increasing

STEP FOUR: Potential risk treatments- how will you manage the risk?

Once the risks have been identified, it is important to outline the courses of action to address these. Possible scenario/solutions:

1. **Avoidance** (**elimination**): Includes not performing an risky activities, i.e changing the travel routes, avoiding areas deemed unsafe, etc.
2. **Reduction** (**mitigation**): Involves methods that reduce the severity of the loss e.g. equipping staff with health and safety kits, keeping emergency numbers, fire equipment, backing up files, etc.
3. **Retention:** Involves accepting the loss when it occurs.
4. **Transfer:** Means causing another party to accept the risk. This can be typically done through insurance, outsourcing services, etc.

These strategies work best when combined.

TIP: *Develop, monitor, and communicate written policies and procedures to all stakeholders so that they are aware of paths of mitigation.*

STEP FIVE: Create a risk management plan

Select appropriate controls or countermeasures to measure each risk. The mitigation needs to be approved by the appropriate level of management

Table 3: Sample risk management table

Description of risk	**O**	**S**	**Rank**	**Status**	**Action**	**Who**	**Cost**
Looting of property	low	medium	2	New possibility	Insure all property		
Loss of staff members	medium	high	1	Increasing	Periodical security alerts issued to staff		

This example is brief; more detail should be added as required.

STEP SIX: Implementation

Follow all the planned methods for mitigating the effect of the risks.

STEP SEVEN: Evaluate and review

Initial plans are never perfect or wholly effective. Experience and change in circumstances will necessitate changes in the plan and contribute information to allow different decisions to be made depending on the risk being faced.

***TIP**: A successful risk management strategy is one that is tailored to your organization. It is up to you to design a strategy that is realistic given the resources of your organization and any other limitations you may face*

SAMPLE RISK MANAGEMENT REGISTER

Description of risk	Likelihood of occurrence	Level of seriousness	Status	Action	Who	Estimated cost
Employees						
Death of staff members	Medium	High	Increasing	• Set up a compassionate fund		
Injury to staff				• Periodic security alerts issued to staff • Health insurance		
Inability to access areas of operation						
Property						
Looting of property	Low	Medium	New possibility	Insure all property		
Damage and destruction						
Clients (OVC)						
Increased number of vulnerable						

children						
Volunteer						
Injuries and bodily harm						
Death						
Inability to access areas of operation						
Board members						
Death						
Injuries						

NB: This is a guiding document aimed at helping you think through the issues and should be tailored to suit organization.

Once the team has gone through the evaluation of the risks and has come up with remedial strategies, a simple risk management framework can be outlined as follows:

SAMPLE OUTLINE OF THE RISK MANAGEMENT FRAMEWORK

Organization XYZ

Risk Management Policy and process

Date

1. Risk to assets/equipment/property

1.1. Safety precautions

- Do you have a fire extinguisher on site?
- Do you have a first aid kit on site?
- Do you have 24 hour security?
- Do you have an alarm response mechanism in place?
- In case of a security breech, who will be contacted?

1.2. Inventory

- Do you have a current property inventory list? (office and furniture)
- Do you have more than one copy of the inventory list?
- Where are copies of the inventory list kept?

1.3. Computer records

- Do you back up your main server/hard drive?
- How often do you back up your system?
- Do you have more than one back-up copy?
- Where are the back-ups kept?
- Do all staff back up their individual files onto CD-Rom?

1.4. Storage of furniture and equipment

- Who is the staff property coordinator in charge of equipment inventories, liability, and storage?
- Who is responsible for arranging storage for furniture and equipment in case of temporary or long-term closure of office?

1.5. Contents of the safe

- Who keeps an inventory of the contents of the safe (such as petty cash, checkbooks, and important records?)
- In case of emergency, where will the checkbooks and important documents be kept?

1.6. Important documents

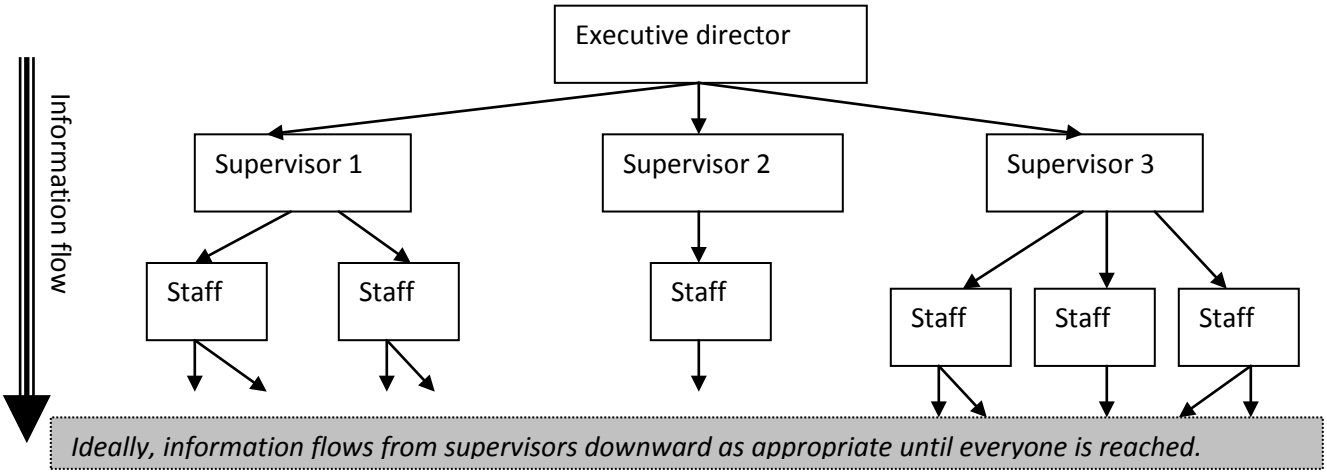
- Where are copies of project contracts, cooperative agreements, leases, insurance policies, database records (with backup diskettes), and registration documents kept?

1.7. Keys

- Do you have a complete set of duplicate keys?
- Where is the set of duplicate keys kept?

1.8. Personnel telephone line and communication strategy

- Does every member of staff have an updated telephone list of all local staff and important telephone numbers (such as hospitals, police emergency numbers, ambulance services, etc.)?
- Do you have an established communications system that defines the chain of communication in case of emergency? Draw up a communication tree. Example:



1.9. Property insurance

- Is your property insured?
- Where are copies of the insurance policies kept?

2. Risk to Personnel

2.1. Chain of command

- What is the order of command in the organization in case of emergency? I.e., if the executive director is incapacitated, who will be the acting team leader? And if that person is incapacitated, who is next in line? (Up to three levels).

2.2. Signatories on bank accounts

- Who are the signatories to your accounts?
- In case of an emergency, do you have alternative signatories to the accounts?

2.3. Manuals of procedures

- Do you have complete manuals for important office procedures?

2.4. Cross training

- Are all staff familiar with basic office procedures?

2.5. Security procedures

- In the event of heightened security levels, what procedures are in place to secure staff safety?