RISK MANAGEMENT MANUAL

PIDF SECRETARIAT

Pacific Islands Development Forum

LAST UPDATE: 10TH JUNE 2016

PREPARED BY: VILIAME KASANAWAQA- TL POLICY RESEARCH AND EVALUATIONS

CHECKED BY: PENIJAMINI LOMALOMA- DEPUTY SECRETARY GENERAL

APPROVED BY: FRANÇOIS MARTEL– SECRETARY GENERAL

`

TABLE OF CONTENTS:

DISTRIBUTION:

1. Secretary General PIDF
2. Deputy Secretary General PIDF
3. PIDF Team Leaders

OBJECTIVE:

To define the organization and responsibilities to enhance the quality and utilization of Risk Management Systems and deliverables and to integrate risk based thinking into PIDF institutional practice.

Version	Date	Object of the update	Prepared by	Checked by	Approved by
0	10/06/2016		TL Policy Research and Evaluations	Deputy Secretary General	Secretary General

OBJECTIVES

The principles of risk management are very basic. Risk is a function of the probability of an event happening and the consequence or severity if that event did happen. It is then only a degree of complexity to which this principle is then applied. Logically, if decisions are made that reflect the principle of risk management (as defined above), then better business decisions will result.

REFERENCES

1) AS/ NZ 4360- Risk Management Standards. Retrieved June 2016 from http://infostore.saiglobal.com.
2) ISO 3100. Retrieved June 2016 from www.iso.org
3) Program Management (Fundamentals of Project Management). Michel Thiry. Gower Publishing.
4) Risk Analysis and Management: Evaluating and Managing Risk. Retrieved June 2016 from www.mindtools.com/pages/article/newTMC_07.htm.
5) QMS Policy OF PIDF

ABBREVIATIONS

M&E- Monitoring and Evaluation

ISO- International Standards Organization

NDC- Nationally Determined Contribution

NSDB- National Sustainable Development Boards

PIDF- Pacific Islands Development Forum

QAI- Quality at Implementation

QMS- Quality Management System

SDG- Sustainable Development Goals

TLPR&E- Team Leader Policy Research and Evaluation

ToR- Terms of Reference

RISK MANAGEMENT

Whatever your role in Pacific Islands Development Forum, it's likely that you'll need to make a decision that involves an element of risk at some point. Risk is made up of two parts: the probability of something going wrong, and the negative consequences if it does. Risk can be hard to spot, however, let alone prepare for and manage. And, if you're hit by a consequence that you hadn't planned for, costs, time, and reputations could be on the line. This makes Risk Analysis an essential tool when your work involves risk. It can help you identify and understand the risks that you could face in your role. In turn, this helps you manage these risks, and minimize their impact on your plans. This manual articulates the risk management procedure for the Pacific Islands Development Forum Secretariat Staff, consultants and contractors.

Risk Management in Programmes

According to Michel Thiry, risk in project management is associated with a lack of information which leads project teams to make assumptions and thus cause risks. In program management, Thiry argues that risk is brought about by the ambiguity of the expectations versus the defined requirements.

Program risk management focuses on the risks that will affect the strategic outcome and benefits of the program and thus must be assessed at a program level. The risks in the program can be classified into 3 classes namely, program risks, project risks and aggregated risks.

Program risks

These risks affect the entire program and are brought about by uncertainty and ambiguity to the program by lack of data or of the unknown unknowns.

Project risks

This group of risks refers to risks associated to a particular project within a program. These risks are addressed through the individual project risks management by the project teams.

Aggregated Risks,

The aggregated risks refers to similar risks that occur through a number of projects within the program thus require to be addressed at a program level as they have the possibility to affect the entire program.

WHAT IS RISK ANALYSIS?

Risk Analysis is a process that helps you identify and manage potential problems that could undermine key business initiatives or projects. To carry out a Risk Analysis, you must first identify the possible threats that you face, and then estimate the likelihood that these threats will materialize. Risk Analysis can be complex, as you'll need to draw on detailed information such as project plans, financial data, security protocols, marketing forecasts, and other relevant information. However, it's an essential planning tool, and one that could save time, money, and reputations.

WHEN TO USE RISK ANALYSIS?

Risk analysis is useful in many situations:

- When you're planning projects, to help you anticipate and neutralize possible problems.
- When you're deciding whether or not to move forward with a project.
- When you're improving safety and managing potential risks in the workplace.
- When you're preparing for events such as equipment or technology failure, theft, staff sickness, or natural disasters.

- When you're planning for changes in your environment, such as new competitors coming into the market, or changes to government policy.

HOW TO USE RISK ANALYSIS?

To carry out a risk analysis, follow these steps:

1. Identify Threats

The first step in Risk Analysis is to identify the existing and possible threats that you might face. These can come from many different sources. For instance, they could be:

Threats Identification Table

1	Human – Illness, death, injury, or other loss of a key individual.
2	Operational – Disruption to supplies and operations, loss of access to essential assets, or failures in distribution.
3	Reputational – Loss of customer or employee confidence, or damage to market reputation.
4	Procedural – Failures of accountability, internal systems, or controls, or from fraud.
5	Project – Going over budget, taking too long on key tasks, or experiencing issues with product or service quality.
6	Financial – Business failure, stock market fluctuations, interest rate changes, or non-availability of funding.
7	Technical – Advances in technology, or from technical failure.
8	Natural – Weather, natural disasters, or disease.
9	Political – Changes in tax, public opinion, government policy, or

	foreign influence.
10	Structural – Dangerous chemicals, poor lighting, falling boxes, or any situation where staff, products, or technology can be harmed.

Table 1 Threats Identification Table

You can use a number of different approaches to carry out a thorough analysis:

Run through a list such as the one above to see if any of these threats are relevant.

Think about the systems, processes, or structures that you use, and analyze risks to any part of these. What vulnerabilities can you spot within them?

Ask others who might have different perspectives. If you're leading a team, ask for input from your people, and consult others in your organization, or those who have run similar projects. Tools such as SWOT Analysis and Failure Mode and Effects Analysis can also help you uncover threats, while Scenario Analysis helps you explore possible future threats.

2. Rate the Risk

Once you've identified the threats you're facing, you need to calculate out both the likelihood of these threats being realized, and their severity. One way of doing this is to make your best estimate of the probability of the event occurring, and then to multiply this by the amount it will cost you to set things right if it happens.

Risk Rating = Likelihood x Severity

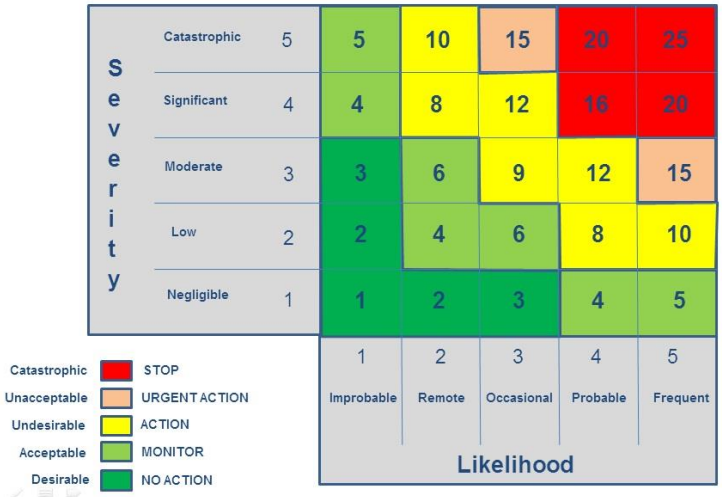

Table 2 Risk Rating

This gives you a Rating for the risk:

Risk Rate = Likelihood of Event x Cost of Event

How to Manage Risk

Once you've identified the value of the risks you face, you can start to look at ways of managing them.

Tip:

Look for cost-effective approaches – it's rarely sensible to spend more on eliminating a risk than the cost of the event if it occurs. It may be better to accept the risk than it is to use excessive resources to eliminate it. Be sensible in how you apply this, though, especially if ethics or personal safety is in question.

Avoid the Risk

In some cases, you may want to avoid the risk altogether. This could mean not getting involved in a business venture, passing on a project, or skipping a high-risk activity. This is a good option when taking the risk involves no advantage to your organization, or when the

cost of addressing the effects is not worthwhile. Remember that when you avoid a potential risk entirely, you might miss out on an opportunity. Conduct a "What If?" Analysis to explore your options when making your decision.

Share the Risk

You could also opt to share the risk – and the potential gain – with other people, teams, organizations, or third parties. For instance, you share risk when you insure your office building and your inventory with a third-party insurance company, or when you partner with another organization in a joint product development initiative.

Accept the Risk

Your last option is to accept the risk. This option is usually best when there's nothing you can do to prevent or mitigate a risk, when the potential loss is less than the cost of insuring against the risk, or when the potential gain is worth accepting the risk.

For example, you might accept the risk of a project launching late if the potential sales will still cover your costs.

Before you decide to accept a risk, conduct an Impact Analysis to see the full consequences of the risk. You may not be able to do anything about the risk itself, but you can likely come up with a contingency plan to cope with its consequences.

Controlling Risk

If you choose to accept the risk, there are a number of ways in which you can reduce its impact. Business Experiments are an effective way to reduce risk. They involve rolling out the high-risk activity but on a small scale, and in a controlled way. You can use experiments to observe where problems occur, and to find ways to introduce **preventative** and **detective** actions before you introduce the activity on a larger scale.

Preventative action involves aiming to prevent a high-risk situation from happening. It includes health and safety training, firewall protection on corporate servers, and cross-training your team.

Detective action involves identifying the points in a process where something could go wrong, and then putting steps in place to fix the problems promptly if they occur. Detective

actions include double-checking finance reports, conducting safety testing before a product is released, or installing sensors to detect product defects.

Plan-Do-Check-Act is a similar method of controlling the impact of a risky situation. Like a Business Experiment, it involves testing possible ways to reduce a risk. The tool's four phases guide you though an analysis of the situation, creating and testing a solution, checking how well this worked, and implementing the solution.

		Level of risk			
		Low	Medium	High	Extreme
Control effectiveness	Fully effective		9	8	2
	Substantially effective		22	44	12
	Partially effective		9	42	22
	Largely ineffective		4	12	15
	None or totally ineffective			5	2

Table 3 Control Effectiveness Rating

Risk Rating After Evaluation of Controls						
(C) Control Effectiveness → / Risk Rating Before Controls ↓	1	2	3	4	5	Risk Rating After Evaluation of Control $R_1=R_0 \times C$
1	1	2	3	4	5	Low Risk =C (1 to 16)
2	2	4	6	8	10	
3	3	6	9	12	15	
4	4	8	12	16	20	
5	5	10	15	20	25	
6	6	12	18	24	30	
8	8	16	24	32	40	Moderate Risk (ALARP)=B (16 to 43)
9	9	18	27	36	45	
10	10	20	30	40	50	
12	12	24	36	48	60	
15	15	30	45	60	75	High Risk =A (43 & above)
16	16	32	48	64	80	
20	20	40	60	80	100	
25	25	50	75	100	125	

Table 4 Risk Classification after Controls Implementations

METHODOLOGY OF RISK ASSESMENT

- Identify Risk as per Risk Assessment Table 1 and Log into Risk Register and identified risk.
- Determine initial risk rating (before implementation of controls) using Tables 2 and update Risk Register
- Write down existing controls applicable for Threat under consideration and update Risk Register.
- Rate control effectiveness using Control Effectiveness Rating (Table 3).
- Re-evaluate the risk rating for the threat using the Risk Classification Matrix after Controls Implementation (Table 4).
- Identify future controls require & update "further actions required" in the Risk Register.

IMPLEMENTATION OF IDENTIFIED CONTROLS

Once the controls are identified for risk elimination and/or treatment of the risk, action plans will be prepared to address the implementation of these controls in a phase wise manner.

The detailed action plans will be submitted to the Team Leader of the responsible Unit for his approval and necessary budget provision. Implementation of identified controls will be tracked and/or reviewed on a six monthly basis by the Executive Management.

The Risk Assessment process must be undertaken prior to the implementation of any major operational changes within PIDF.

It is the responsibility of the Unit Team Leader of the area concerned to initiate the Risk Assessment process.