Appendix C

RISK RESPONSE PLANNING : SELECTING THE RIGHT STRATEGY

Crispin ("Kik") Piney

kik@PROject-beneFITS.com

Overview

For project risk management to be carried out effectively, all of the steps – from Risk Management Planning, through Identification and Analysis, to Response Planning and finally Monitoring and Control (PMI "PMBOK®", 2000) – need to be integrated consistently in line with the project objectives and the risk tolerances of the organization and the stakeholders. Where a number of potential responses are available for dealing with any given risk, an agreed method is required in order to select the preferred approach, to support with the wider business strategy – for example, how to decide between the option of taking out insurance and that of accepting the risk. The paper will show how to develop and use an integrated decision tool, known as the Project Risk Response Chart.

Organisational Risk Tolerance

Utility concepts

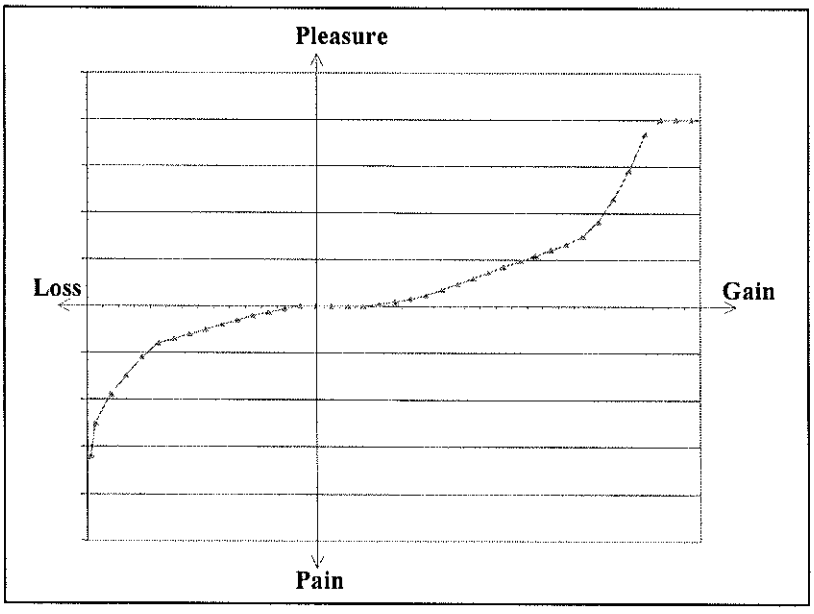
To quite a large extent, the potential impact of risks (whether they are opportunities or threats) is a subjective matter. However, in all cases, we can identify three main ranges of impact (fig. 1 below is taken from: Piney, 2002):

- Where the effect can be ignored ("dead zone")
- Where the effect rises at the same rate as the size of the impact ("rational zone")
- Where the effect rises very sharply once the size of the impact exceeds a given threshold ("sensitive / saturation zone")

A simple example of this is given by the way in which you might reason about playing a lottery. If the ticket is very cheap, you might buy it just for the fun of it – "you won't miss the money". If the ticket costs more, you would then calculate whether the potential prize makes playing worthwhile (for example by comparing the expected monetary value of the prize against the price of a ticket). Beyond a given price, you would not agree to buy a ticket, whatever the prize.

This relationship between (objective) cost and (subjective) value (or pain) can be represented by a "utility curve", as shown in Fig.1.

Fig. 1: Utility Curve for Gains and Losses

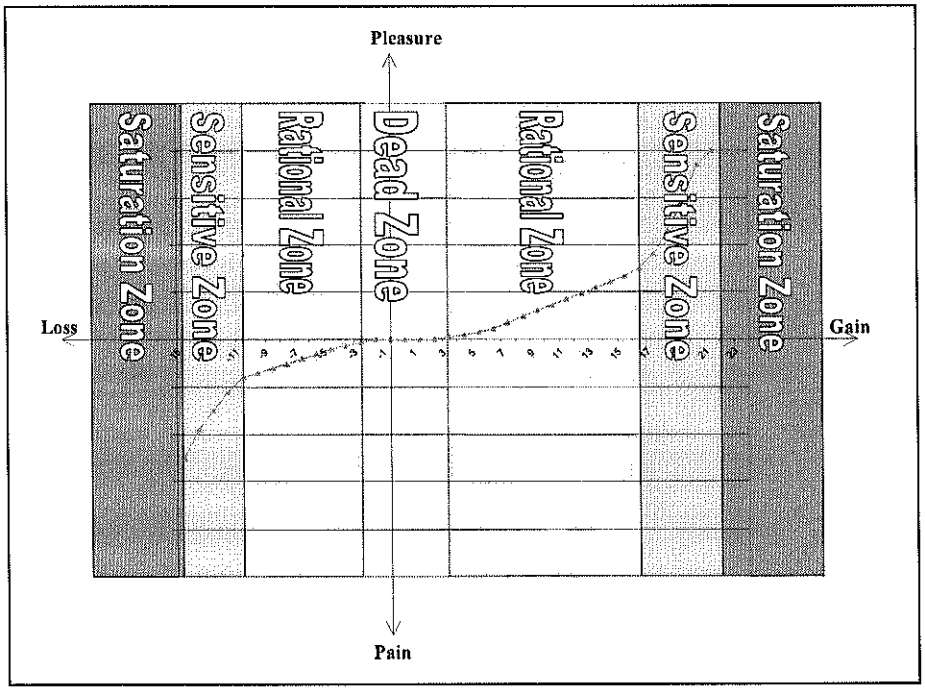


The vertical axis represents "utility units" which can be chosen either as "percentage of maximum imaginable" or some other unit that effectively measures the subjective effect of a given impact.

A brief inspection of the curve shows that each half (pleasure – for opportunities – and pain – for threats) has four distinct areas (as shown in Fig. 2), starting from the origin, and delimited by an abrupt change in the slope of the utility curve:

- An area where the impact is considered insignificant ("dead zone")
- An area where the utility varies linearly with the impact ("rational zone")
- An area where the utility varies increasingly rapidly with respect to the impact ("sensitive zone")
- An area where the utility bears no relationship to the corresponding impact: for opportunities, it reaches a ceiling of pleasure, whereas, for pain, it goes to infinity ("saturation zone")

Fig. 2: Utility Curve for Gains and Losses



In order to obtain the curve, the way in which risk is viewed by a business or organization needs to be understood. This depends on a large number of factors, such as:

- Financial conditions of the company: large multi-national, down to small business
- Business approach: from steady, safety-conscious long-established company to aggressive, risk-taking start-up.

These organization-related features have to be integrated with the specific characteristics of the project, in order to provide clear guidance for the management of the corresponding risks – e.g.:

- Project budget
- Financial and/ or strategic benefits of the project
- Duration or time-horizon for the project activities to be managed.

One other factor that needs to be defined is a "benchmark": this is the value (see Dembo & Freeman, 1998) of the project outcome which is "expected". In other words, a lower value will generate "regret" (even if it still returns a profit), whereas a higher value will be considered a success. The impacts of the project risks will need to be calculated relative to this benchmark result. In fig. 1, the zero of the x-axis (loss-gain axis) corresponds to this benchmark value.

The Risk Management Plan

The Risk Management Plan (PMBOK®, 2000) describes how risk identification, qualitative and quantitative analysis, response planning, monitoring and control will be structured and performed during the project life cycle. A typical table of contents for this plan is given below:

Fig. 3: Typical Risk Management Plan Structure

Introduction
Methodology
Roles & Responsibilities
Budgeting
Timing
Use of Tools ○ **Scoring and Interpretation** ○ **Thresholds**
Reporting Formats
Tracking and Recording

The "use of tools" section of the Risk Management Plan should contain information relative to the utility parameters for the specific project:

- The project success benchmark
- The limiting values of the various utility zones shown in fig. 2 with, if possible, the utility curve itself
- The Risk Response Planning Chart that is described in the following sections

These will be of use for both analysis and response planning.

Once you understand the way in which risk should be viewed within the context of your project, you are in a good position to develop the guidelines with respect to which the potential responses will be assessed.

Risk Response Planning

Risk Response Planning entails developing options and determining actions to enhance opportunities and reduce threats to the project's objectives. A clear explanation of the appropriate approach is given in Hillson 1999. There are four main categories of response strategies for threats: avoidance, transfer, mitigation and acceptance. The corresponding strategies for opportunities (see also Hillson, 1999 & 2001) are: exploit, share, enhance and ignore. When carrying out the planning and subsequent selection of the primary response, the project manager needs to know the conditions under which each strategy will be considered to be acceptable, required, or unacceptable for the specific project. The potential responses need to be assessed with respect to the effect they have on three key parameters:

- The expected value of the outcome (i.e. the product of impact by probability, plus the cost of the response)
- The worst case scenario (i.e. the impact plus the cost of the response)
- The best case scenario (i.e. the event does not occur: take the response impact into account)

Response planning for threats

The PMBOK® identifies four different approaches for responding to risks. These are explained briefly below, along with their main characteristics plus an insight into how these characteristics interact with risk thresholds defined in the Risk Management Plan. This serves as the basis for developing a synthesis view to be known as the Risk Response Planning Chart.

As explained in Hillson 1999, some risks may require a combination of strategies.

Risk avoidance

Risk avoidance entails taking actions so that the risk event no longer impacts the project objectives. This can be achieved either through changing the way of carrying out the relevant activities or by modifying the objectives. If avoidance can be achieved for little or no cost, that approach should obviously be taken. On the other hand, avoidance will be mandatory if the potential impact (after all valid attempts to reduce it) remains unacceptable i.e. the impact falls beyond a point on the utility curve, defined in the Risk Management Plan.

Risk transfer

Risk transfer implies ensuring that a third party will shield the project – totally or in part – from the impact of the risk event. This will normally require a financial arrangement ("risk premium") between the project and the third party – e.g. an insurance premium, a financial guarantee, a contract provision, etc. Generally, risk transfer will have the following effect on a chance event: it will make the "best case" scenario less good, the "worst case" scenario less bad and displace the expected monetary value towards lower benefit. This approach is therefore to be preferred in the case where a bad "worst case" would cause more damage than the potential reduction in the "best" and "expected" values, as measured on the corresponding utility curves.

Risk mitigation

This is a general term for reducing probability and/or consequences of an adverse risk event. In the extreme case, this can lead to eliminating the risk entirely (as seen in "avoidance").

However, in mitigation, it is not sufficient to consider only the resultant expected value, because, if the potential impact is above a certain threshold - given in the Risk Management Plan -, the risk remains unacceptable. In this case, one of the other approaches will have to be adopted.

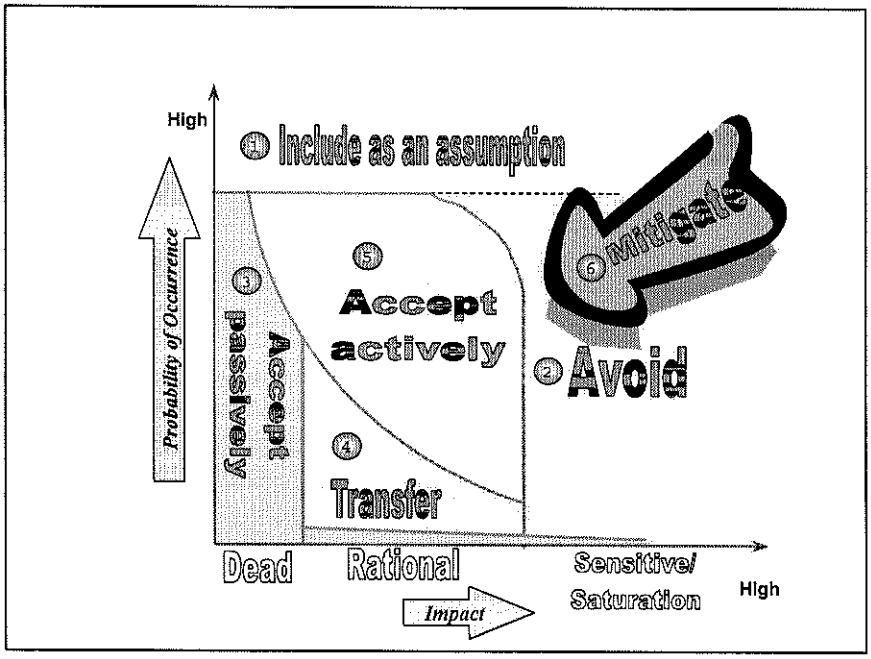
Risk acceptance

Risk acceptance entails planning for ways in which to deal with the event if it occurs, rather than attempting to influence its probability or impact. From the point of view of the project, this will be the strategy of choice in cases where the effect of the risk is known to be sufficiently contained for it to be acceptable (i.e. below the defined "pain threshold"). Acceptance can be "passive" when the impact is of minor importance (e.g. in the utility "dead" zone); in this case, no prior plans are put in place. Acceptance is "active" when the impact, if the event occurs, will need to be reduced: in this case a "contingency" plan for responding to the event is developed so as to reduce the overall impact (cost of the plan plus cost of the risk event) to an acceptable level.

Building the risk response planning chart for threats

All of these guidelines for selecting the category of response can be represented on a single chart as shown below: each area (1-5) on the chart defines the primary strategy that should be considered for any risk that falls within that area; mitigation (6) is treated as a potential adjunct to each of these strategies. The overall shape of a risk response planning chart is the same for all projects. However the values and scales of the axes will change depending on the organisation and the project.

Fig. 4: Typical Risk Response Planning Chart for Threats



The rationale behind the chart is as follows:

1. Above a given probability of a risk, it is often easier to manage the situation by assuming that the event will happen and treating its non-occurrence as a potential opportunity
2. All risks with an impact over a given limit can totally wreck a project: they all have to be *avoided* except at a vanishingly small probability
3. All risks with an impact in, or near the utility "dead zone" (and within the tolerances of the project) can be *accepted passively*
4. Between passive acceptance and avoidance, some action has to be taken. If the frequency of occurrence of a risk is low (i.e. gives an expected value below a chosen value within this range of impacts), it is not worthwhile for the project organisation to put effort into a contingency plan; it should therefore *transfer* the risk.
5. For risks that are more likely to occur – and potentially a number of times –, it is beneficial for the organisation to plan for the eventuality by *accepting actively*, and save the corresponding risk premium.
6. In addition, *mitigation* should be used wherever it proves viable, to move the risk towards the lower expected values

Using the risk response planning chart for threats

The way in which the chart should be used is as follows:

a) Using the results of the risk analysis phase, identify where the risk falls in the chart
b) Ignore any risks in the "ignore" area
c) Apply mitigation where viable
d) Apply the response strategy that corresponds to the mitigated risk. Note that you can select the strategy from the region in which the risk falls, or that of any region corresponding to a risk of greater expected value, if the cost of the strategy is acceptable.

This is shown in more detail in the flowchart in fig. 5.

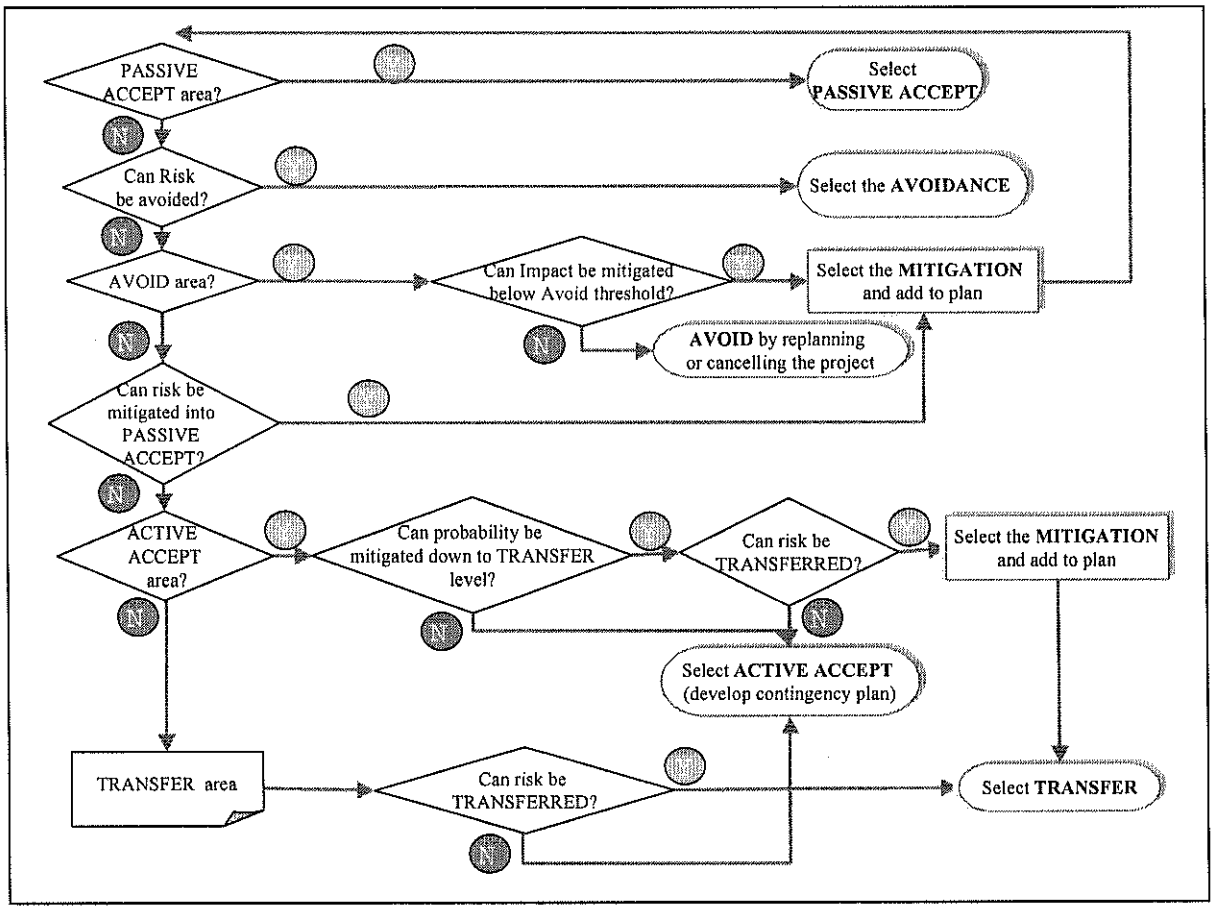


Fig. 5: Flowchart of risk response planning actions for Threats, based on where a threat falls in the Risk Response Planning Chart

You should then:
e) Identify and analyse the risks introduced by any changes to the previous plan ("secondary risks")
f) If any secondary risks are outside the "passive accept" area, restart at a) for the "secondary risks"

Risk Response planning for opportunities

As explained earlier, each of the response strategies for threats has a corresponding strategy for opportunities. These can be mapped onto the utility regions in the same way as for threats, giving rise to the chart shown in fig.6, and the flowchart in fig.7.

Fig. 6: Risk Response Planning Chart for Opportunities

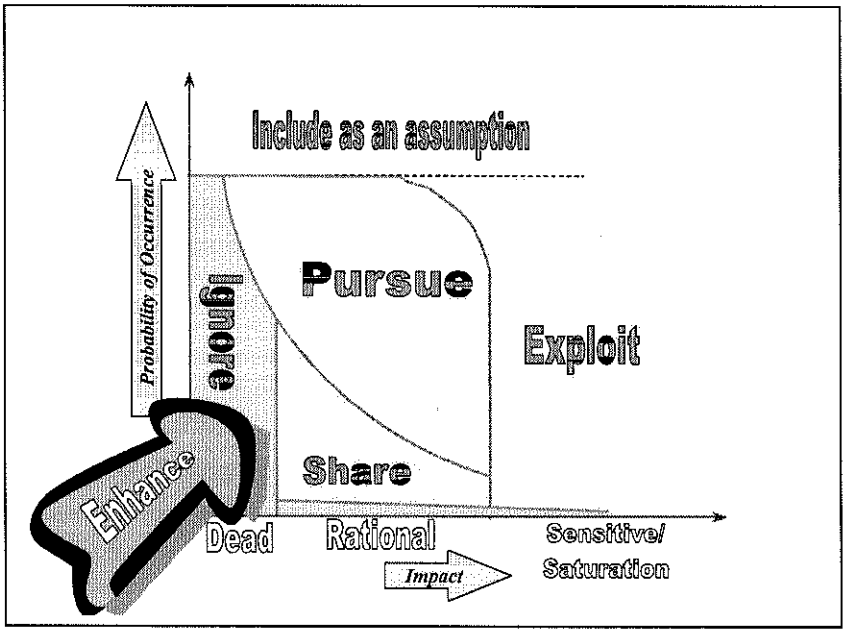
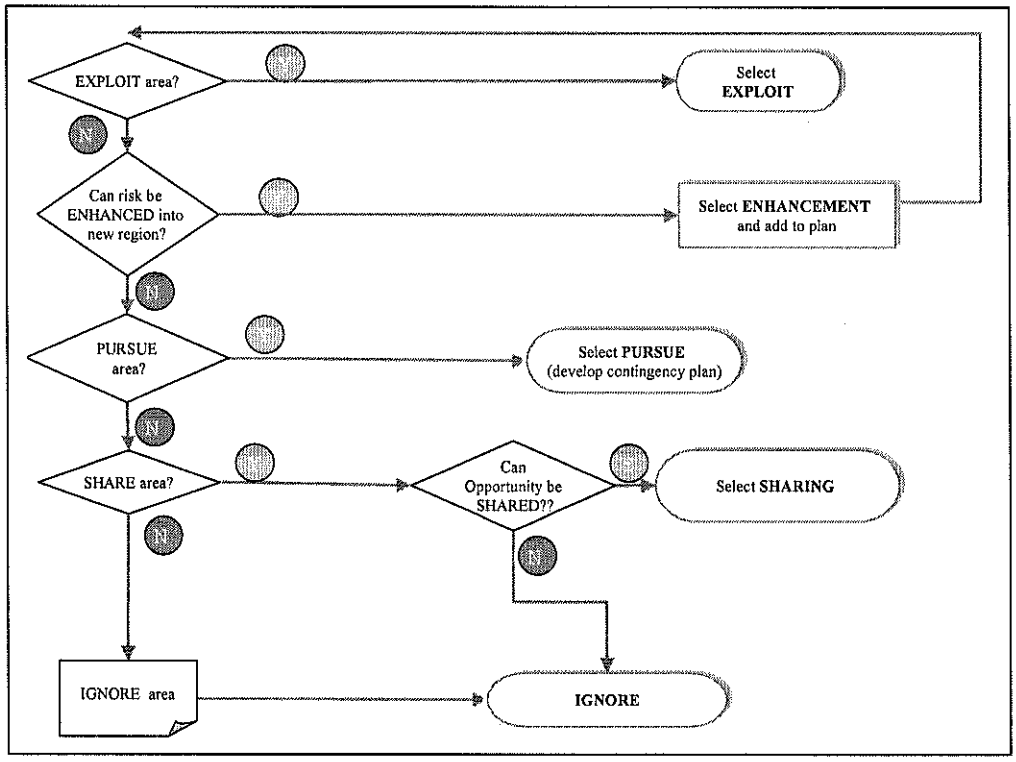


Fig. 7: Flowchart of risk response planning for Opportunities



Risk Response Planning Example

This example demonstrates the way in which the threat flowchart and analysis rules can be used. It also shows how response actions can interact as well as generating new risks.

Consider the project to install an automated voice response telephone service in a call centre in order to support an organisation's after-sales service business. The threats identified are

A) Total loss of service due to failure of the voice switch
B) Financial loss due to fire in a voice switch
C) User dissatisfaction due to reduced human interaction

Risk C falls in the *passively acceptable* area and nothing will be done about it.

Risk A falls in the unacceptable (i.e. *avoid*) area. We decide to modify the design to include batteries to eliminate stoppage due to power failure, and to double-up the equipment to mitigate equipment failure.

Risk B falls between "passive" and "avoid"; we can see no way of mitigating it down to "passive acceptance"; the probability of fire is low, so we will *transfer* the risk by insuring it.

Our actions have raised secondary risks:

D) If a power outage is too long, the batteries will be run down, leading to loss of service. This risk has been increased by doubling-up on the equipment, since the batteries will drain twice as fast. We need a contingency plan (*active acceptance*) that includes use of power generators
E) There is the risk that the insurance company will be unable (or unwilling) to pay in case of fire. This is considered so unlikely as to be *accepted passively.*

Our responses to the secondary risks have raised more risks:

F) The cost of running the power-generators could damage the business forecast. We will partially *transfer* the impact by including a penalty clause in our agreement with the electricity supplier.

There now remain no risks that are insufficiently contained.

Conclusions

By establishing the thresholds of acceptability of the impact and probability of risks at the start of the project, the subsequent tasks of risk response planning can be carried out in a structured and predictable way that has a high chance of complying with the business objectives and constraints of the sponsoring organisation.

References

Books:

Dembo, Ron S.; Freeman, Andrew. 1998. *Seeing Tomorrow.* NY, NY: John Wiley & Sons.

Project Management Institute, 2000. *A Guide to the Project Management Body of Knowledge.* Pennsylvania: PMI.

Articles:

Hillson, David. 1999. Developing Effective Risk Responses. *Proceedings of the 30th Annual Project Management Institute 1999 Seminars & Symposium.*

Hillson, David. 2001. Effective Strategies for Exploiting Opportunities. *Proceedings of the Project Management Institute Annual Seminars and Symposium Nashville, Tenn., USA.*

Piney, Crispin ("Kik"). Submitted 2002. Applying Utility theory to Risk Management. *Project Management Journal.*

Contingency Plan Template for Any Business	Version 1.0 8 May 2006	Author: Robert Lengyel, Director, Brains for Business. www.brains.com.au	Form BCP01

Purpose of this document	This document provides a template that could be used to construct business contingency plans for **Any Business.**
Follows Australian and International Standards	This template is aligned with the features and principles outlined in Australian Standard HB 221:2004 "Business Continuity Management" and follows principles outlined by the International Disaster Recovery Institute.
Practical Application and Use of this Template	This template is a realistic working tool that has been used by the author to create in excess of 1 000 business continuity plans for many different organizations throughout Australia. It has "stood the test of time" and been found to be of great practical benefit to those organisations that have used it.
Design and features of this document	This document contains instructions for the construction of business contingency plans for the widest range of hazards and risks. Complex jargon has been avoided and sample data is provided alongside most areas where the BCP creator is required to provide information. The author's basic template can be slightly redesigned to reflect the operating environment and characteristics of **Your Business.**
Sample Plans Included	Two sample plans have been included where this template has been filled in with real life data from a pathology laboratory business for the loss of power and the absence of telecommunications for the laboratories.
Why Use a Template for Constructing Business Contingency Plans?	A template provides a standardised method for constructing plans and other documents. A uniform approach for BCP construction is encouraged and supported by a BCP template that is used across **your whole Business**. A template does away with the need for an in depth "skill up" for a BCP project, and if used correctly, ensures that a standard format and rigor is applied to the business contingency plan creation process.
Other Documents to be used	This document should be used in conjunction with form BCT01, "Testing Template for Testing Business Contingency Plans".

Some important terms explained

Business Continuity Management	Provides for the availability of processes & resources in order to ensure the continued achievement of critical business objectives.
Business Continuity Plans	Consist of a collection of procedures & information that is developed, compiled & maintained in readiness for use in the event of an emergency or disaster.

Title: **Failure of xxxxx** *(Insert name of critical resource, e.g. telecommunications, power etc.)*

*Remember that different sections of **Your Business** will react differently to a common disruption as their critical business functions will be different than yours. This means that you should NEVER use the same business contingency plan (for example 'Loss of power or telecommunications") for different business units or sections!*

Location: **Primary Site** *(the location where this plan will be actioned and stored)*

Plan ID: **XXXNN** *(the plan identification number, e.g. CSBCP01)*

Plan Purpose:

Outline the steps that should be taken in the event of the loss of a particular resource or service. *(E.g. The steps to be taken for loss of power to this building).*

Distribution List:

Provide a list of people who have copies of this plan and their location and contact details.

Responsible Personnel:

Define who has overall responsibility for all resources and services of the system in the event of failure and who will be directing the response and recovery. *(This would normally be the business unit manager).*

Also list the person/s will ensure that all required actions are performed by qualified personnel. *(This may also be the business unit manager, or a higher level manager who has overall responsibility for delivery of this business unit's service or output).*

Reasons for failure:

Determine the reasons for failure:

- Identify the possible reasons for failure in priority order

(Determining the reasons for failure will assist you in deciding how long the disruption will last and help to determine the extent of the disruption. E.g. for a power failure the reasons could be partial failure of power because of local circuit problems, failure of power to the whole building, street or suburb, town or city etc).

Warning Indicators:

- Identify warning signs or indicators of failure. *(E.g. for a loss of power it might be room lights not working, internal phone lines not working. Your response and actions will be determined by what has actually gone wrong or failed and how long it will take to fix the problem).*

Areas Affected:

Identify areas that are affected:

- List areas that may be affected *(This refers to functional work areas as well as physical areas of the Department. E.g. contact with the rest of Your Business may be affected, contact with clients, data entry, scheduled important meetings, urgent reports, as well as areas like this room, the building, the entire office floor etc.)*

Recovery Time Objective (RTO):

State the recovery time objective:

(This is the time up to which the system is monitored and after which the plan is implemented in order to prevent serious business impact)

(This can be expressed in units of minutes, hours, days, weeks etc. For example, an air traffic controller system may have a RTO of 5 minutes because that is the minimum time they can operate without their system before a serious business impact occurs. For a taxi dispatch system the RTO may be 1 hour).

Your response here will be in the form of: 1 hour or 5 minutes, 1 day etc.

Notification:

Call for assistance and notify personnel *(Consider placing contact phone numbers and other details here or in an attachment page).*

Internal

- List personnel Internal to the site to be notified in priority order *(This may be business unit manager, front office staff, switchboard operators etc. Note that you may need to notify a person/group who will be charged with spreading your notification message to all other internal staff and you may need a mechanism to ensure that your message will be delivered with clarify and a degree of swiftness).*

External

- List External resources providers and other sites to be notified in priority order *(This will be your business partners or other sections of Your Business who rely on your services or who regularly communicate with you. Your business unit "may be off the air" while you are invoking and carrying out the steps outlined in this contingency plan).*

Make sure you fill in the business interruption contact log attached to your plan. This is to ensure that you have carried out all the necessary steps and to assist you in the recovery phase and provide information when you evaluate your response at a later stage.

Resources for notification

- List resources required for notification *(This may include items such as pages, mobile phones, local phone systems, other plans etc.).*

Backup Resources:

Check and monitor the status of backup resources in priority order. *(Backup resources includes items like a generator, UPS devices, access to document storage etc.).*

Recover backup resources if necessary in priority order.

- List backup resources available (incl. any documents or plans that are referenced)

Initial Response

Determine the estimated duration of failure and compare with Recovery Time Objective

If estimated duration of outage is **less than RTO**, implement - Monitoring tasks.

(The monitoring, initiation and sustaining tasks described below may include those responsible for carrying out the tasks and a suggested time limit that must be complied with for the tasks to be successfully implemented. E.g. the laboratory technician has 30 minutes to place specimens from the pathology machines into the refrigerators in the "event of a power failure". The fridges will be powered by the back up generator. Their task may be slightly different if the disruption goes over the RTO and in the event of "sustaining tasks ", specimens may have to be moved from the fridges and placed in dry ice and eskies and couriers deliver the specimens to other laboratories.)

Monitoring tasks

Responsibility: *Who is responsible for carrying out these monitoring tasks.*

- List monitoring tasks and those responsible for carrying out these tasks

If estimated outage is **greater than RTO**, implement – Initiation tasks

Initiation tasks

Responsibility: *Who is responsible for carrying out these initiation tasks.*

- List initiation tasks and those responsible for carrying out these tasks

Sustaining

Monitor situation and re-evaluate at **X hour intervals.**

After ***Y hours,*** decide if the sustaining tasks listed below are to be implemented.

(For example, every 2 hours we monitor the situation up to 6 hours and we then decide if we then commence the series of "sustaining tasks".)

Sustaining Tasks

Responsibility: *Who is responsible for carrying out these sustaining initiation tasks.*

- List tasks and internal and external personnel to be notified.

Rostering of staff *(If staff need to be rostered or existing changes to roster need to be changed, list what must be done by who.)*

•

Additional resources required *(Outline what additional resource will be required if the disruption continues, e.g. additional couriers, demountable offices, buses to ferry staff to emergency data centre etc.)*

NB. Some sustaining tasks may require the initiation of other business contingency plans. Consider the loss of power where the "Y" sustaining time is 6 hours and the emergency generator will only last for 5 hours, you may have to invoke the BCP for telecommunications failure as your PABX system UPS and your building generator will not power your PABX beyond the 6 hours!

•

Recovery

If confirmed that failure has ended, commence recovery tasks:

Recovery Tasks

Responsibility: *Who is responsible for carrying out these recovery tasks.*

- List the tasks (and the responsible task holders) required for the return to normal operations in priority order, and the internal and external personnel to be notified.

Updates and Plan Location

When implemented, record events on attached Business Interruption Event Log.

Review and update when there are additional or changed conditions specified.

Locations of the plan are specified
A copy of the plan is made accessible to appropriate staff specified.

Business Interruption Event Log

Event Description:			
Location:			
Date	Time	Actioned By	Contact/Task

SAMPLE 2 - Failure of Power Supply Business Contingency Plan

Location: **ABC Private Hospital Pathology Lab**

Plan ID: **ABCH02**

Plan Purpose:

To maintain essential pathology services to ABC Company P/L Hospital for the duration of the loss of power.

Distribution List:

ABC Pathology Lab Manager at the ABC Hospital – phone: 07 3312 3456

HQ Business Continuity Manager – phone: 07 123 4567

Gold Coast Regional Pathology Lab Manager – phone: 07 5512 3456

Responsible Personnel:

The Laboratory Manager or delegate has overall responsibility for recovery of the Laboratory operations as a result of the failure.

A Practice Management Group manager has overall responsibility for maintaining Pathology services to ABC Company P/Private Hospital.

Reasons for failure:

Determine reasons for failure:

- Failure of power supply to the Laboratory
- Failure of power supply to the Wesley Hospital
- Failure of power to the Laboratory rooms only
- Partial failure of laboratory circuits only

Warning Indicators:

- Room lights not working
- Air-conditioning not working
- No Power to instruments
- Blood bank fridge alarms
- UPS alarms
- Internal telephones (PABX) not working

Areas Affected:

Identify areas that are affected:

- Laboratory alone
- Parts of Hospital building
- Entire Hospital

Recovery Time Objective (RTO):

1 hour

(The time up to which the system is monitored and after which the plan is implemented in order to prevent serious business impact)

Notification:

Contact will be by any unaffected means of communication (e.g. Mobile phone, Public Phone, unaffected fax line).

Call for assistance and notify personnel

Internal

- Taringa switchboard operator

Taringa Switch to notify:

- ABC Laboratory Manager
- Practice Management Group (PMG) manager
- Computer operator to advise cause of online equipment disconnection
- Taringa Lab to advise of possibility of redirected work
- Wesley Lab to advise of possibility of blood bank work

External

- ABC Company P/Hospital wards

Resources for notification:

- Telephone as above

Backup Resources:

Check and monitor the status of backup resources in priority order.

Recover backup resources if necessary in priority order.

- The PABX UPS has approx. 15min battery power
- Instrument UPS's have battery power for shutdown only
- Eskies for controls, reagents and blood products
- Dry ice for controls storage
- Ice bricks for reagent storage
- Rechargeable torch

Initial Response

Determine the estimated duration of failure and compare with Recovery Time Objective

If estimated duration of outage is less than RTO, implement - Monitoring tasks

Monitoring tasks

- Shutdown instruments on UPS
- Turn off PCs
- Turn off computer terminals
- Turn off fridges
- Reset blood bank fridge alarm
- Leave lights on to determine when power is restored

If estimated outage is greater than RTO, implement – Initiation tasks

Initiation tasks

- Transfer dry ice to esky and store controls
- Transfer ice bricks to esky and store reagents
- Transfer ice bricks to esky and store blood products
- Notify Practice Management Group (PMG) manager that require couriers and to redirect blood banking and blood products to Wesley Lab, other work to Taringa Lab.
- Implement "Telecommunications failure Contingency Plan; ABCH01"

Sustaining

Monitor situation and re-evaluate at 2-hour intervals in priority order.

After 6 *hours*, decide if sustaining tasks are to be implemented.

Sustaining Tasks

- Notify blood bank staff to proceed to Wesley Lab for shifts
- Notify other staff to proceed to Taringa Lab for shifts
- Notify Hospital of Lab closure and transfer of work to Taringa and Wesley Labs.
- Close laboratory and transfer operations to Taringa Lab.

Rostering of staff

- Liaise with Brisbane Laboratories Manager re rostering of staff.

Additional resources required

- Telecommunications failure contingency plan; ABC01

Recovery

If confirmed that failure has ended, commence recovery tasks:

Recovery Tasks

- Proceed as per telecommunications failure contingency plan
- Turn on equipment and lights
- Restock fridges with controls, reagents and blood products

Updates and Plan Location

When implemented, record events on attached Business Interruption Event Log.

Review and update when there are additional or changed conditions or when work procedures are reviewed.

A copy of the plan is with the ABC lab quality system procedures manual.

A copy of the plan is in the ABC lab manager's office.

Business Interruption Event Log

Event Description:			
Location:			
Date	Time	Actioned By	Contact/Task