CONTEMPORARY APPROACHES TO PROJECT RISK MANAGEMENT: ASSESSMENT & RECOMMENDATIONS

Prepared by:

Mohamed Noordin Yusuff

IT Security Officer

Dip.ECC, SDip.IS, M.IntSecMgmt(Distinction)

INTRODUCTION

In order to manage risks, we have to define what risk is. From the OXFORD dictionary, risk is defined as *"possibility of meeting danger or suffering harm"*. With this definition, it makes us feel that there is a need to avoid risks especially when managing projects. But unfortunately, like what all risk managers know, risk can never be avoided BUT it can be reduced – and that is what management wants to hear. And unfortunately again, risks are often ignored. By abolishing constraints and reducing ambiguities, risk can be minimised to an acceptable level. Project risks may be "accidentally" overlooked by those who just do not have time to look into it or those who want to avoid serious delays. Others may be terrified to look into it because if risks were to be uncovered, the team may look incompetent in managing the project. To manage the risk that has been exposed, there is a need to fix that risk – and to fix that risk, it will cost more *money* – a resource that a project usually lacks. Risk management should be conducted throughout the whole project lifecycle – from the initiation phase till the decommissioning of the project. Risk Management could often contribute to project success through improvements due to the loopholes it uncovered.

APPROACHES TO RISK MANAGEMENT

Organization normally uses three different approaches to risk management:[1]

- Project Management Institute, Project Management Body of Knowledge, Chpt. 11
- UK Association for Project Management Project Risk Analysis and Management (PRAM) Guide
- AS/NZS 4360 Standard

Chapter 11 of the Project Management Body of Knowledge (PMBOK) from the Project Management Institute focuses on Project Risk Management. It includes the following major areas:[2]

[1] Dr Stephen Grey, "Risk Management Processes", (n.d), Retrieved: September 3, 2004, URL: http://www.broadleaf.com.au/publications/Conf_PMI_Melb_Nov_2001.ppt

[2] William R Duncan, "A guide to the Project Management Body of Knowledge", 1996, URL:

- Risk Identification
- Risk Quantification
- Risk Response Development
- Risk Response Control

Risk Identification involves in pinpointing the risks that may affect a project. Risk Identification has to be conducted at regular intervals throughout the life span of the project. Risk Identification has to take into consideration internal and external factors. Internal factors involve risks that the group which is handling the project can manage. Some examples of internal factors are the delegation of work, freezing of vacation leaves and budget allocation. External factors involve risks that the project personnel are not in command of. Some examples of external factors are economic fluctuations, policy restructuring or natural disasters.

Risk Quantification is the assessment of risks and how different risks are linked and communicated with each other, in order to determine the activity required for different risk occurrence. Risk Quantification includes several different aspects:[3]

- Complex calculations may result to incorrect accuracy and consistency.
- Good prospects for one stakeholder may be a downfall for another.
- A risk occurrence can have a snowball effect.
- Chance and ways to exploit this chance communicate in unexpected ways.

Risk Response Development includes preventive measures against threats. These measures fall into one of the below-mentioned categories:[4]

- Avoidance – abolishing a particular danger. This is by abolishing the root of the problem.
- Mitigation – lessening the cost of a risk occurrence by lessening the likelihood of this occurrence.
- Acceptance – to absorb the consequences

---

http://www.projectability.co.uk/downloads/pmbok.pdf

[3] William R Duncan, "A guide to the Project Management Body of Knowledge", 1996, URL: http://www.projectability.co.uk/downloads/pmbok.pdf

[4] William R Duncan, "A guide to the Project Management Body of Knowledge", 1996, URL: http://www.projectability.co.uk/downloads/pmbok.pdf

In order to counter risk occurrences during the entire project life cycle, there is a need to perform Risk Response Control which includes the execution of the risk management plan. PMBOK is a process structure for management understanding. The below-drawn chart substantiates a common understanding of how project risk management is broken down into four sub-groups of risk identification, risk quantification, risk response development and risk response control.

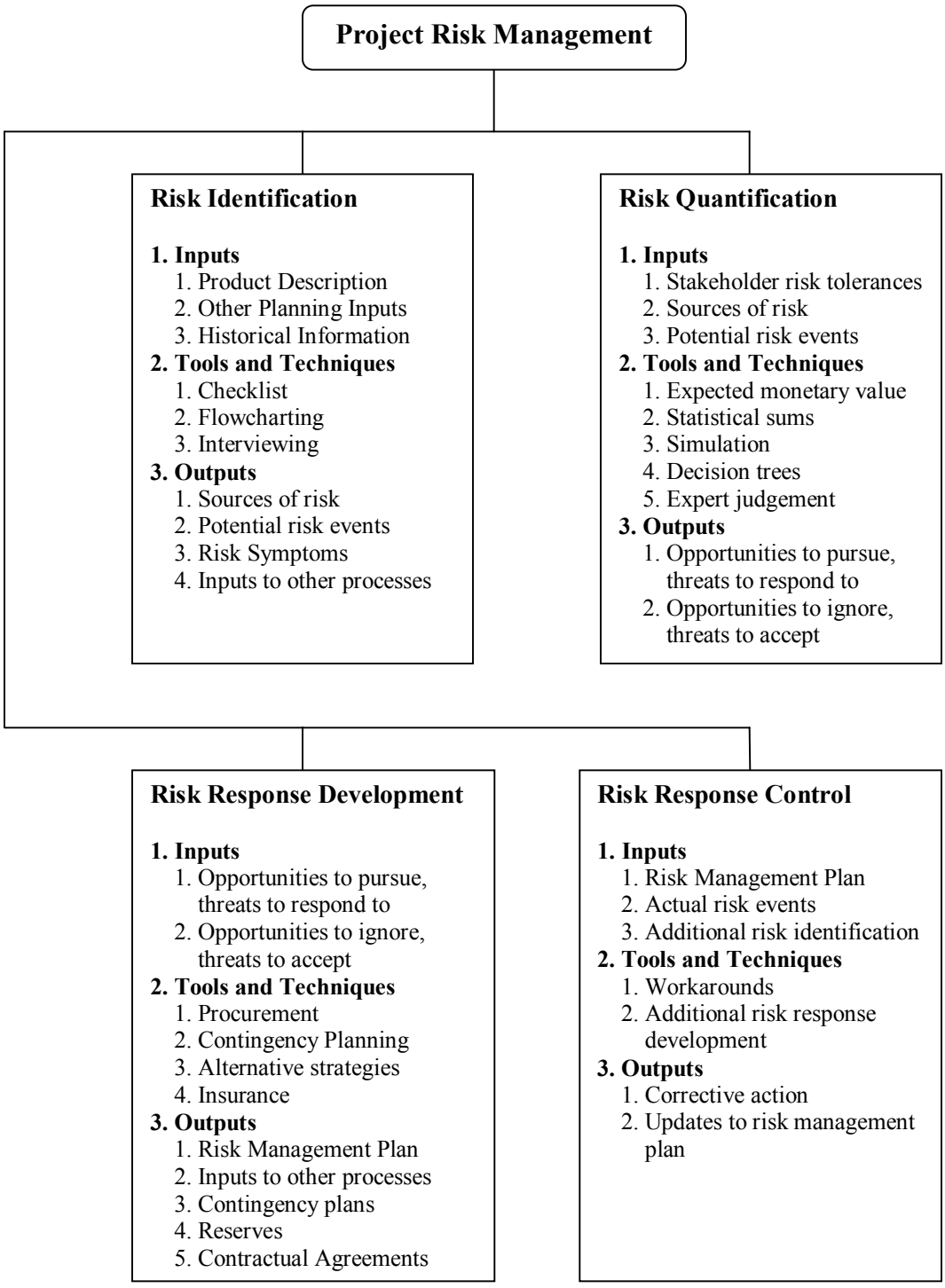

Figure 1: Project Risk Management Overview[5]

[5] William R Duncan, "A Guide to Project Management Body of Knowledge",1996, URL: http://www.projectability.co.uk/downloads/pmbok.pdf

UK Association for Project Management Project Risk Analysis and Management (PRAM) Guide offers a practical framework for users who are new to Project Risk Analysis and Management. It is a method that involves the study and organization of risks pertaining to specific projects. Proper execution of Project Analysis and Management will lead to successful finishing of projects in terms of cost, time and expected performance. PRAM is used to minimise risks that may impact project objectives. This framework is divided into two categories:[6]

- Risk Analysis
- Risk Management

Risk Analysis is further divided into two sub-categories which is qualitative and quantitative analysis.[7] Qualitative analysis involves identifying and recognising risk factors. It is then complemented by an assessment which describes each risk and its impact. Quantitative analysis assists in clearing up doubts involving time and cost estimates, and also individuals' doubts.

Risk Management involves how management responds to risks. It includes:[8]

- recognising preventive measures to minimise risk
- implementing contingency plans to counter risk
- reduce doubts via investigation through useful information
- transfer of risk to another asset
- risk allocations in contractual agreements
- setting contingencies to budget allocations

PRAM is also a structural process for management understanding.

[6] Catriona Norris, Professor John Perry, Peter Simon, "Project Risk Analysis and Management", (n.d.), Retrieved: 3 September 2004, URL: www.eurolog.co.uk/apmrisksig/publications/minipram.pdf
[7] Catriona Norris, Professor John Perry, Peter Simon, "Project Risk Analysis and Management", (n.d.), Retrieved: 3 September 2004, URL: www.eurolog.co.uk/apmrisksig/publications/minipram.pdf
[8] Catriona Norris, Professor John Perry, Peter Simon, "Project Risk Analysis and Management", (n.d.), Retrieved: 3 September 2004, URL: www.eurolog.co.uk/apmrisksig/publications/minipram.pdf

The AS/NZS 4360 standard was developed to accommodate public sector and private organizations on Risk Management. Its risk management approach is very generic. This standard consists of processes as illustrated in the diagram below:

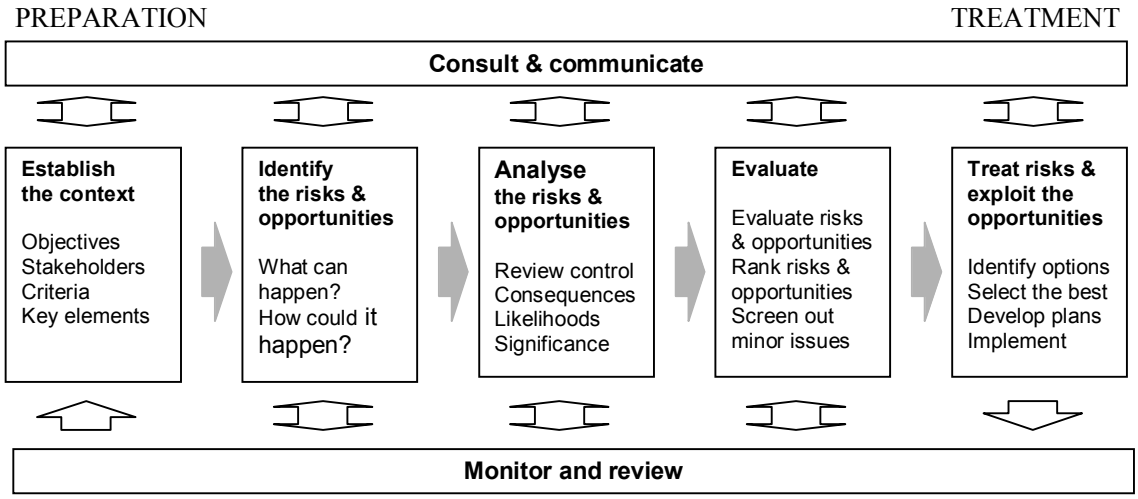

Figure 2: AS/NZS 4360 Structure[9]

This standard is more of a process based rather than a methodology based framework. This methodology is specifically for Risk Management. It can be used in any projects. This methodology is highly structured. Modifications to this methodology would have to be made to suit certain organizations' objectives.

[9] Dr Dale F Cooper, "Tutorial Notes: The Australian and New Zealand Standard on Risk Management",1995, URL: http://www.broadleaf.com.au/tutorials/Tut_Standard.pdf

ADVANTAGES AND DISADVANTAGES

PMBOK – Ch11

This chapter 11 of Project Risk Management is integrated in the Project Management Body of Knowledge. Project Managers adhering to this technique are strongly guided by its detailed processes. One of the disadvantages is that this technique may be quite strenuous and unfair to large projects. Management processes and risk concepts blend in together. It is a cost-effective implementation process.

PRAM

Its risk management techniques are very detailed and precise. There are detailed activities and tasks to adhere to with necessary inputs and expected outputs. With detailed techniques, it strongly guides the user throughout the project lifecycle. This technique allows a direct linkage to the management. However, the risk concepts used are very broad and subjected to numerous discussions.

AS/NZS 4360

This standard is considered rather simple, but easy to adhere. Any type projects could easily follow this framework. It is scaleable and able to support different levels of integration. This standard is accepted worldwide and used in many organizations. This standard has its fair share of disadvantages; it is not implemented to accommodate evaluation of risks.

FROM ORGANIZATION'S PERSPECTIVE

Coming from an organization that mainly manages information technology, our IT projects are mostly software-based to accommodate our end users. Risk Management is done in-house. It is needed to enhance corporate control in terms of allocating resources in a more effective way, improve the ability to look out and utilize opportunities, and also internal or external factors that may affect the organizational success. As a department in a non-profit organization, there is a need to understand that it

doesn't generate any revenue but only spend the amount of budget allocated on different projects. However, careful planning is always undertaken to minimise risks and take advantage of opportunities. Coming from an organization that focuses very much on security and adhere to policies or standards that are internationally recognised, the AS/NZS 4360 standard with relevant adjustments is highly recommended for the Project Teams to adhere.

The AS/NZS 4360 Risk Management standard specifically handles risk. A reasonable amount of time is required to collate necessary information. The AS/NZS 4360 standard had also since been adopted by the Australian Government and large organizations. This standard was also developed to apply risk management in public sector and private sector organizations. As only a small team conduct risk management for all projects, inputs have to be obtained by the relevant project teams. Though using the AS/NZS 4360 standard, as a government organization, there is a need to come up with a proprietary internal Risk Management Methodology addressing the IT projects. The above-drawn standard has to be strictly adhered with extra adjustments. There are many risk events that affect a particular project but sometimes these risks focus more towards the operational aspect of a project such as "*why does this particular page takes very slow to upload"* but rather risk management have to include information and data security which is a very important aspect and must be adopted in its methodology. There is also a need to assess different controls that are already in place for a particular project, and work out if there needs to be more. Risks have to be valued according to its criticality. When it comes to risks, threats and vulnerabilities of a particular project have to be identified. Controls for the risks have to be put in place. This Risk Assessment Workgroup or steering committee will determine the risk treatment in terms or mitigation, acceptance or transference, thus monitoring and reviewing the Risk Management process. An owner would have to be assigned to carry out the action plan and define the expected completion date for the implementation of controls. The below-drawn diagram is a recommended example of how a government organization can adopt a security-focused risk management methodology based on AS/NZS 4360 standard. As a government organization, processes have to be strictly adhered and there must be accountability on

the performance generated by a particular project. That is why there is risk management to look into performance issues.

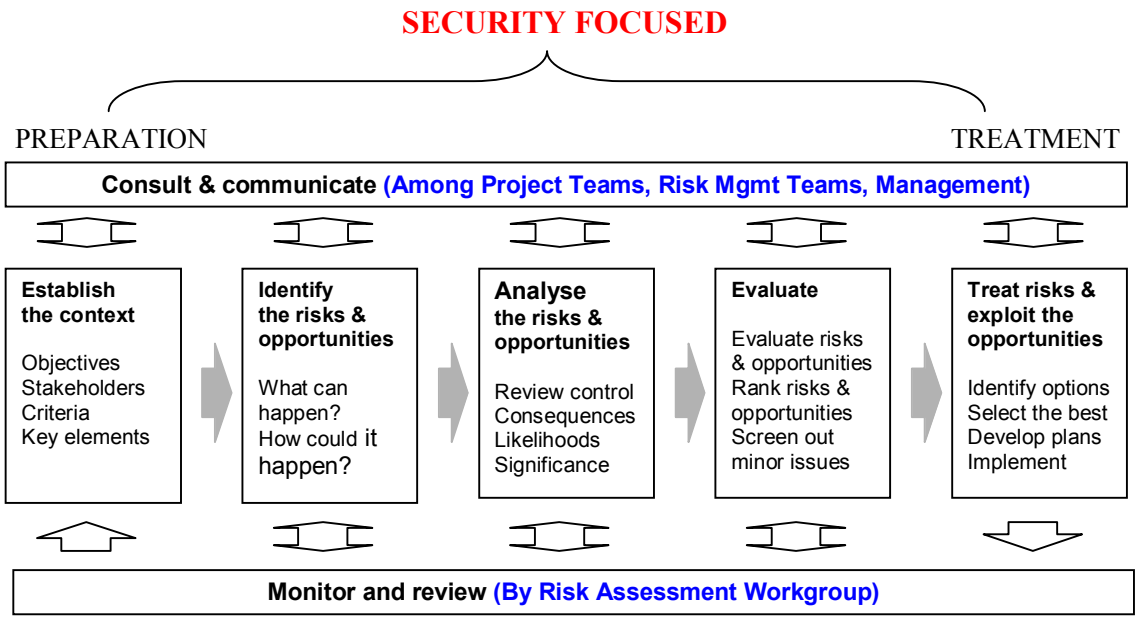

Figure 3: AS/NZS 4360 Structure[10] **with *Recommendations***

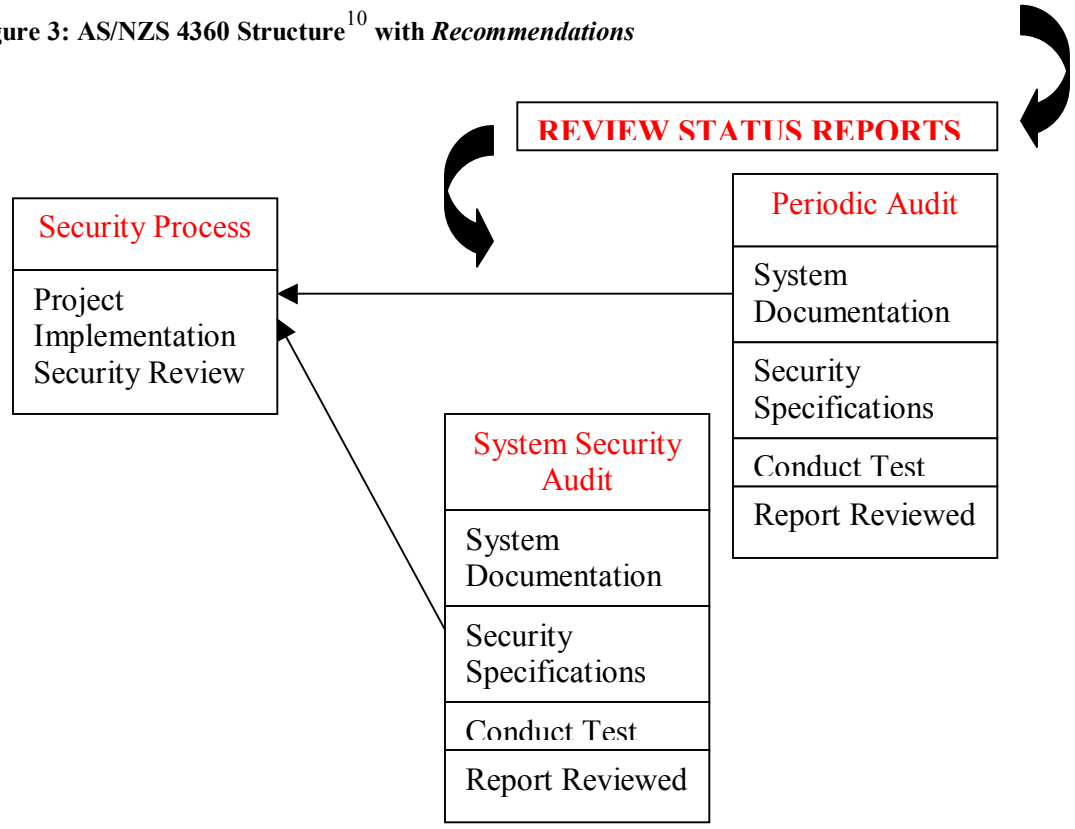

Figure 4: Recommendations on Security Process for Risk Management

[10] Dr Dale F Cooper, "Tutorial Notes: The Australian and New Zealand Standard on Risk Management",1995, URL: http://www.broadleaf.com.au/tutorials/Tut_Standard.pdf

Figure 4 concentrates on Security during the Risk Management process. Security has to be taken into consideration during the implementation of projects. Before the project goes into production, there will be a System Security Audit to ensure that all security measures have put into place and the system is secure After which, there will be a periodic assessment to ensure that all risk controls remain intact. Status reports on projects have to be submitted before moving on to the Security Process stage. This standard needs to ensure the presence of commitment from management, managers and project teams. All risks and opportunities are identified through this recommended standard. The implementation of this standard is very cost-effective. Sufficient resources have to be allocated. The risks and controls are addressed in terms of severity thus allowing priorities to be set. The Return-On-Investment is bountiful because government organizations have their own team of Risk Management experts to lead this process. For external audit, third party services will need to be engaged. The only investment that the organization has to make is paying salaries to the staff. Though this standard is detailed, it suits a government organization where risks are controlled, budgets are maintained and security is the first priority.

ORGANIZATIONAL ISSUES ON RISK MGMT APPROACHES

Sometimes, management in the organization do not play a proactive role when it comes to risk management. This have to change as there must be directions from the top to ensure the success of a particular project. Communication between top management, middle management and project teams have to be two-way. There needs to be a feedback from both sides on their opinions about a particular project to ensure success and to ensure that everything that is done on that particular project is within scope. For example, requirements and directions come from the management where as required resources or incidents come from the staff. Projects have to be monitored throughout its lifecycle. To allow monitoring, it can be tracked through a tracking system detailing updates about the project. Project reviews or status updates to the management have to done monthly for necessary directions. Normally, project managers are sent for training, and the organization uses *"Train the trainer"* technique to educate their staffs. This is not an

efficient technique; there is a need to ensure common understanding among managers and their staff. Risk can come and go at different times. Risk Management is always regarded as a one-time thing in an organization; it have to be regarded as a continuous process throughout the project lifecycle. Using the AS/NZS 4360 standard, there needs to be inputs from the staff and project managers. There is also a need to understand that though there is an internal risk management team doing risk management for projects; there is a need for third-party audits to assess whether the risk has been managed without any favouritism. Third-party audits will incur costs, but most importantly is that management must understand the importance and objectives of the third party audits. Sometimes, staff and management give a negative attitude towards risk management as they might think it as a *"finger-pointing process"* or *"blaming session"*. This culture should change. Risk Management should be thought of as a technique towards achieving project excellence. By adopting the AS/NZS 4360 standard, work procedures have to be changed and staffs have to be trained. There may need to allocate extra resources in certain areas. This AS/NZS 4360 standard should be incorporated during the phase when the project is being planned. Though cultural change might take time and consistent planning, the management must play a part in constantly communicating or deliver the policies to their staffs, thus raising awareness and achieve a common understanding in this arena of Project Risk Management. Management must support risk management.

The usage of PMBOK and PRAM is rather similar. Though, it is quite easy to comprehend, it may not be entirely fulfilling organizations' risk management needs. These methodologies address both management and risk concerns. But for a non-profit or even government organization, these two methodologies are rather hectic for staffs to comply.

CONCLUSIONS

Risk Management is always forgotten when managing projects but the irony is that all projects have risk. People in general think that risk management is just a blaming session to uncover flaws in a particular project. This perception has to be abolished. Management and Project managers have to understand that Risk Management is the one of the few practical way to manage uncertainties and doubts towards a particular project.

Risk can never be abolished, but can only be reduced to an acceptable level. Risk Management is a must for any projects and it has to be done from the initiation phase throughout the project lifecycle. Risk Management is not free, and it isn't cheap – There may need to have third party audits which incur cost. There must always be continual management support and commitment to ensure the success of projects.

As mentioned above and referenced accordingly, there are 3 major approaches to Risk Management - *PMBOK Ch11, PRAM and AS/NZS 4360 Standard*. Different organizations or even different Project and Risk Managers adopt different techniques of Risk Management. Some may adopt it with necessary modifications to suit the environment of their organization. A non-profit or government organization, for example may adopt a Risk Management standard such as AS/NZS 4360 Standard but with certain modifications (as described above) to suit the organization's objectives. But, the organization must really choose what kind of risk management strategy suits them. Most importantly there must be continual management support and commitment throughout the project lifecycle.

Lastly, Risk Management has to be adopted during the project initiation phase, throughout the project lifecycle. The project must also be monitored and reviewed to look out for further risks involvement. Organizational culture need to change and accept Risk Management as part of their daily work, rather than a one-time *thingy*.

REFERENCES

Robert Tusler, "An Overview of Project Risk Management", 29 July 1996, URL: http://www.netcomuk.co.uk/~rtusler/project/riskprin.html

Preston G. Smith, Smith CMC, Guy M. Merritt, "Managing Consulting Project Risk", 3 September 2002, URL: http://www.newproductdynamics.com/Risk/C2M9-02.pdf

Preston G. Smith, "Thirteen ways to mismanage development project risk", 2002, URL: http://www.newproductdynamics.com/Risk/Visions7-02.pdf

Alquier A.M., Cagno E., Caron F., Leopoulos V., Ridao M.A., " Analysis of external and internal risks in project early phase", (n.d.), Retrieved: 3 September 2004, URL: http://www.esi2.us.es/prima/Papers/PRIMA_art2.pdf

Preston G. Smith and Guy M. Merit, "Dealing with Project Risks Successfully", October 2002, URL: http://www.newproductdynamics.com/Risk/PDBPR-Risk.pdf

Dr Dale F. Cooper, "Implementing Risk Management Processes", 30 May 01, URL: http://www.broadleaf.com.au/publications/Conf_PubSec_Bne01_RM.pdf

Project Management Institute, "A Guide to Project Management Body of Knowledge", 2000, URL: http://www.pmi.org/prod/groups/public/documents/info/pp_pmbokguide2000excerpts.pdf

William R Duncan, "A guide to the Project Management Body of Knowledge", 1996, URL: http://www.projectability.co.uk/downloads/pmbok.pdf

Catriona Norris, Professor John Perry, Peter Simon, "Project Risk Analysis and Management", (n.d.), Retrieved: 3 September 2004, URL: www.eurolog.co.uk/apmrisksig/publications/minipram.pdf

Dr Dale F. Cooper, "Tutorial Notes: The Australian and New Zealand Standard on Risk Management", (n.d.), Retrieved: 3 September 2004, URL: www.broadleaf.com.au/tutorials/Tut_Standard.pdf

Dr Stephen Grey, "Comparison of three approaches to project risk management", (n.d.), Retrieved: 3 September 2004, URL: http://www.broadleaf.com.au/publications/Conf_PMI_Melb_Nov_2001.ppt

Dr Dale F. Cooper, "Implementing Risk Management: Organization and Cultural aspects of risk management", (n.d.), Retrieved: 3 September 2004, URL: http://www.broadleaf.com.au/publications/CAE_Nov_03_COOPER_Organisational_and_Cultural_Aspects_of_RM_Implementation.pdf