

## **A Framework for Risk Management Practices and Organizational Performance in Higher Education**

Mohd Shoki Bin Md. Ariff\*  
Norhayati Zakuan  
Muhammad Naquib Mohd Tajudin  
Azira Ahmad  
Faculty of Management,  
Universiti Teknologi Malaysia, Malaysia  
Email: m-shoki@utm.my

Nawawi Ishak  
Lembaga Tabung Haji, Malaysia

Khalid Ismail  
Universiti Pendidikan Sultan Idris, Malaysia

— *Review of* —  
**Integrative  
Business &  
Economics**  
— *Research* —

### **ABSTRACT**

Risk management is recognized as a prominent aspect of the good corporate governance of a successful institution. The need for effective risk management framework is widely recognized by academic and industry to manage all type of risks encountered by an organization. However, managing risk practices in the not for profit arena, including public higher education institutions, appear to be significantly less developed as compared to that of business world. In Malaysia higher education scenario, some public universities are awarded autonomous status, and therefore, a framework for effective management of risks is needed. Review of literature related to risk management indicated that Enterprise Risk Management (ERM) framework is a best practice and can be applied in higher education setting. However, the risk management framework of ERM need to be costumed to suit the unique mission, risk context and risk profile of higher education. Based on the review of literature and ERM framework of COSO and ISO 31000:2010, risk governance, risk policy, risk context, risk treatment, communication and consultation, risk identification, risk analysis, risk evaluation, and monitoring and review of risk management process, tools and technology, and continuous improvement of the risk management practices, is proposed for the public universities. Organizations that have implemented systematic risk management practices are enjoying high level of organizational performance. However, specific measure of performance is needed to link the risk management practices and the impact on the organizational performance. A review on organizational performance measures related to risk suggesting that the financial and non-financial performance would serve as construct of organizational performance for these universities. Hence, this study proposes a framework for risk management practices and organizational performance for managing risk in the higher education setting, particularly for Malaysia's public universities with autonomous status.

**Keywords** –Risk Management; Organizational Performance; Higher Education.

## 1.0 INTRODUCTION

Higher education is recognized for pioneering and leading trends, exploring new knowledge, promoting new ideas, and transforming innovation that can be turned successfully and practically to business, industry and community, however, it is far behind business and industry in developing and implementing a practical and sustainable enterprise – wide risk management (ERM) (Tufano, 2011). The National Association of College and University Business Officers (NACUBO) released a report on managing risk in higher education in 2003 that encouraged higher education leaders to implement and advance effective risk management programs (Tufano, 2011). In 2007, three leading higher education associations - The University Risk Management and Insurance Association (URMIA), the Association of Governing Boards of Universities and Colleges (AGB) and the National Association of College and University Business Officers (NACUBO) – published white papers highlighting a strong recommendation for institutions of higher education to go beyond the mere discussion of ERM and start implementing it on their campuses. Higher education institutions should consider risks as part of their strategic planning process (Association of Governing Boards of Universities and Colleges and United Educators, 2009). ERM can be beneficial for universities in addressing key areas of risk being faced by universities and manage the risks that lead to achieving the universities' key performance indicators (Helsloot and Jong, 2006, Tufano, 2011). It could minimize the consequences of unfavourable events and it would motivate the decision-making process to ensure specified organizational performances are met (Zadeh, 2010).

Despite the existence of a rich literature in the fields of risk management, there is little written about risk management practices in relation to the provision of higher education (Tufano, 2011). In Netherland, higher education institutions still do not routinely have an integrated policy related to risk management (Helsloot & Jong, 2006). In Malaysia, the introduction of University Good Governance Index (UGGI) in 2011 requiring public universities to implement an organized risk management for it to get the autonomy status. Currently, five public universities – Universiti Teknologi Malaysia, Universiti Kebangsaan Malaysia, Universiti Sains Malaysia, Universiti Malaya and Universiti Putra Malaysia - were granted the autonomy status since 2012. Operating in new environment after being awarded the autonomous status, these universities are competing intensely in higher education market, which resulted in greater exposure of multi-dimensional risks. The challenge involves uncertainty about future government funding, increasing number of post-graduate students, and the pursuit for high ranks in world university ranking, intense competition in getting quality of international students, and global competition. This provides a great challenge for the universities to explore a framework of risk management and organizational performance that is workable within these universities. A question arises, despite the existence of risk frameworks and approaches, and difficulty to implement ERM in higher education, what is a practical risk management framework for these Universities? Within the framework, the issue is what are risk management practices suitable for managing risk in the above scenario of the universities?

Integration of risk management and performance management is important. Organizations that practice risk management in an integrated manner generate better information for decisions thereby improving on the achievement of their objectives (COSO, 2004). Risk management is not only about reducing or eliminating risks, it's also about

assessing whether achieving your organization's mission requires that you intelligently and mindfully take on greater risk (Tufano, 2011). It is very crucial, to connect risk management straight away with the objectives outcomes at each stage of the organization. Different measure or organizational performance is required to link risk management practices and their impact on the performance. Since no study has been carried out to address risk management framework in higher education, particularly in Malaysia's public autonomous universities status, this research gap must be filled. The question is what constructs of organizational performance for these universities, and do the risk management practices significantly affect the performance of the universities?

## **2.0 LITERATURE REVIEW**

### **2.1 Concept of risk and risk management**

Risk is defined as 'effect of uncertainty on objectives and it aids decision making by taking account of uncertainty and its effect on achieving objectives and assessing the need for any action' (MSISO 31000:2010). Risk management refer to the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects (MS ISO 31000:2010). ERM is a process, affected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (COSO, 2004). In the context of higher education, ERM is a university-wide risk management process applied in strategic setting across the university, designed to identify potential events that may positively or negatively affect the university, and designed to manage the risks so they are within the university's risk appetite, thus contributing to the achievement of university's mission, key performance indicators and objectives.

### **2.2 Risk management framework**

Review on ERM implementation in service industry indicated that COSO integrated framework of risk management (COSO, 2004) and ISO 31000:2009 are widely employed by service firms. These frameworks of risk management describe principles, practices, generic guideline and processes involved in managing risks. ERM is capable of unifying concerted effort and risk management practices to establish risk context and parameter, identify risks, analyse the risk and develop the profile for the risks, and determine risk treatment strategy. However, a tested model of risk management through academic researches and procedures for the higher education is nonexistence. Analysis on the usage of COSO (2004), ISO 31000:2009, AS/NZS 31000:2009 and MS ISO 31000:2010, as depicted in Table 1, contributed to the development of the risk management practices in higher education.

Several variables of risk management processes mentioned in the literature/standards that have been referred to in this paper. These processes of risk management practices are part of the overall framework of managing risk. Table 2 highlighted the outcome of the literature review related to the development of risk management framework (Azira, 2014).

Undisputed standardization on risk management should be enforced in order for the minimal compulsory method of risk management could be applied. Hence, risk management standards, for example COSO and ISO 9001:2009 could be considered when designing a

framework for managing risk. Based on the review of those standards, as depicted in Table 1, the risk management practices of risk management framework that should be considered include (i) risk governance, (ii) risk policy, (iii) risk context, risk identification, risk analysis, risk evaluation, risk treatment, communication and consultation, and monitoring and review of risk management process, (iv) tools and technology, and (v) continuous improvement. Risk management tools, and approaches have been developed to implement proper risk management practices and increasing success (Kwak & Stoddard, 2004). Therefore, in Malaysia's public autonomous universities, all of these risk governance; policy, risk management processes, tools and technology, and continuous improvement are hypothesized to have positive and significant effect on risk management practices.

Table 1: Risk management of COSO, ISO 31000:2009/AUS/NZS 31000:2009, MS ISO 9001:2010 and their contribution towards risk management practices for higher education

COSO (2004)	ISO 31000:2009/AUS/NZS 31000:2009/ MS ISO 31000:2010	Proposed Risk Management Practices
Objective Setting Internal Environment, Environment, process and information	Mandate and commitment Design of framework for managing risk	1. Risk governance
-	Risk policy	2. Risk Policy statement
Event Identification Risk Assessment Risk Response Control Activities Information and Communication Monitoring	Implementing risk management – the processes are identical with what being addressed in AS/NZS 4360:2007 (2004).	3. Risk Management processes – Risk context, risk assessment (risk identification, risk analysis, risk evaluation), risk treatment, communication and consultation, monitoring and review.
Tools and techniques	Tools and techniques	4. Tools & technology
Not specifically addressed in the framework, but it is mentioned in the standard	Continuous improvement of the framework	5. Continual improvement of Risk Management framework

Table 2: List of researchers on Risk Management Processes

Researchers/Standard	Risk Context	Risk Identifica tion	Risk Analysis	Risk Evaluati on	Risk Treatm ent	Risk Consult ation	Risk monitoring & Review
MS ISO31000:2010	/	/	/	/	/	/	/
Kululanga and Kuotcha (2009)		/	/	/	/		/
Chapman (1997)		/					
Tchankova (2002)		/					
Cerevon (2006)		/					
Ahmad et. al (2007)			/	/	/	/	
Kinch et. al (2007)			/				
Elkington et. al (2010)				/			
Lee and Azlan (2002)		/		/	/		

In addition, organisations themselves should create their own framework of risk methodology, approach, practices, and guideline in managing the risk. Therefore, based on review of past researches related to risk management, the following processes of risk management practices should be considered: risk context, risk identification, analysis and

evaluation, risk treatment, risk consultation and risk monitoring and review. A proactive risk management process enables managers to practice proper risk management, and to resolve potential problems before they occur and therefore, contributes to success (Kwak & Stoddard, 2004; Dey et al. 2007). Therefore, in Malaysia's public autonomous universities, all of these risk management processes are hypothesized to have positive and significant effect on risk management practices.

## **2.2 Construct of Risk Management Practices**

### **2.2.1 Risk Governance**

In implementing risk management, governance, policy and procedures for predicting, evaluating and managing risk are important. According to the International Risk Governance Council (2005), risk governance includes the totality of actors, rules, conventions, processes and mechanisms and is concerned with how relevant risk information is collected, analyzed and communicated, and how management decisions are taken. Within this definition, it requires organizations to clearly define how strategic decisions are made taking into consideration of risks, risk management framework, role and responsibility, structure and governance with regard to organizational wide risk management implementation. It also involves specifying commitment and involvement of relevant parties and mandate to be given to those who are directly and indirectly involve in the risk management implementation.

### **2.2.2 Risk Policy**

Risk policy is a statement of the overall intentions and direction of an organization related to risk management (MS ISO 9001:2010). Risk policy provides general guideline for risk management implementation. Typical risk policy statement includes organizational commitment towards risk implementation, objectives, strategy and proactive measures of risk, risk category, the use of organizational wide risk management framework, and continuous improvement of the framework.

### **2.2.3 Risk Management Process**

Based on the MS ISO 31000:2010, risk management process involves establishing the context, risk assessment, risk treatment, monitoring and review, and communication and consultation. In risk assessment, three activities are involved, namely risk identification, risk analysis and risk evaluation. The following section discusses all of these risk management processes.

#### **2.2.3.1 Establishing Risk Context**

This process involves defining and establishing the objectives, strategies, scope and parameters of the activities of the organization, or those parts of the organization where the risk management process is being applied (MS ISO 31000:2010). Relevance internal and external factors affecting the risk management process must be considered and incorporated in the risk criteria and parameter developed. This process is important because it provides

clear objectives and scope of risk management in relation to the organization (Salman and Zain Ul-Abideen, 2010).

### **2.2.3.2 Risk Assessment (Risk Identification, Risk Analysis and Risk Evaluation)**

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation (MS ISO 31000:2010). It is considered to be the most important step for risk management because it provides a base for the right future work of the organization concerning the developing and the implementation of new programs for the risk control (Tchankova, 2002). Risk identification requires organizations to identify sources of risk, areas of impacts, events and their causes and their potential consequences in order to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives (MS ISO 31000:2010).

According to Kutsch, Browning, and Hall (2014), after risk are identified, they must be analyzed to determine which risk are most urgent and most in need of management attention. Risk analysis is performed to understand characteristics of the identified risk and it provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods (MS ISO 31000:2010). Risk analysis is done to determine the identified risks and their characteristics whether they are worth of further analysis (Ahmed *et al.*, 2007).

In reference to the outcome of risk analysis, risk evaluation is executed to differentiate the level of risk that is present during the analysis process with risk criteria or parameter established, in which risk treatment can be based on (MS ISO 31000:2010). In risk evaluation, different mitigation options are determined keeping in view the risk events and then most suitable option is incorporated to the risk mitigation plan (Ahmed *et al.*, 2007).

### **2.2.4 Risk Treatment**

Risk treatment involves selecting one or more options for modifying risks, and implementing those options (MS ISO 31000:2010). Common risk treatment strategy includes actions to reduce the likelihood, reduce the consequences; to transfer the risks, accept or avoid/terminate the risk (AUS/NZS 31000:2009). Risks can be treated either through proactive approach or through reactive approach. Reactive approach refers to the actions initiated after the eventuation of the risks events while proactive approach refers to actions initiated based on chance of the occurrence of certain risks (Ahmed *et al.*, 2007).

### **2.2.5 Communication and Consultation**

The whole process of risk management requires healthy contributions from all the participants within the organization (Ahmed *et al.*, 2007). Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process (MS ISO 31000:2010). Li, et.al. (in Salman and Zain Ul-Abideen, 2010)

suggest that this process of risk management involves expanding internal communication as well as with the stakeholders. Formal internal communication channels must be established and all information related to the risk management implementation must be communicated and displayed to all staff, especially those who are directly or indirectly involved in the risk management process. The continual communication and consultation with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance, is part of good governance (MS ISO 31000:2010).

### **2.2.6 Monitor and Review**

Monitoring and review of the risk treatment plan and implementation should be planned and carried out regularly (MS ISO 31000:2010). It is an essential step in risk management process where risks are properly monitored and the effectiveness of risk treatment plan is reviewed (Salman and Zain Ul-Abideen, 2010). Risk management is a dynamic process, therefore the risk management process needs to be regularly repeated, so that new risks are captured in the process and they are effectively managed (Salman and Zain Ul-Abideen, 2010).

### **2.2.7 Tools and Technology**

Risk management tools, techniques and system should be used to carry out the risk management process and all activities related to the planning, implementing, reviewing and reporting, and continuous improvement of the risk management framework, for example, use of risk dashboard, template, monitoring sheet, risk management information system, etc. As mentioned in MS ISO 31000:2010, organizations should apply risk identification tools and techniques that are suited to their objectives and capabilities, and to the risks faced.

### **2.2.8 Continual Improvement of the Risk Management Framework**

This part of risk management focuses on continual improvement in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills (MS ISO 31000:2010).

## **2.3 Organizational Performance Measures**

Companies that have implemented certain risk management techniques and practices are enjoying high performance (Salman and Zain Ul-Abideen, 2010). In their study, measure of organizational performance related to information technology project include avoiding software project disasters, including run away budgets and schedules, defect-ridden software products, and operational failures. Construct of organizational performance for financial institutions include market growth, credit impact and percentage of profit (Tufano, 2011).

For managing risk in research and development, the Balanced-Score Card (BSC) approach was used for a balanced performance measurement system that is connected with the corporate strategy and has much broader perspectives to enhance performance of the research and development projects (Wang J. et al., 2010). This approach links the financial,

customer, internal process and learning and growth of a university BSC to risk management practices. Thus, the BSC of the autonomous public universities of Malaysia provides key performance indicators for measuring university performances with regard to risk management. Review of key performance indicators of the BSC and risk parameter in these universities (e.g. <http://www.utm.my>) indicated that the institution is pursuing a number of financial (financial perspective) and non-financial (customer, internal process and learning and growth) key performance indicators. According to the Phase 2 of Malaysia's National Higher Education Action Plan (2011), finance and wealth generation is one of the four sections in the assessment of autonomous status procedure under the University Good Governance Index (UGGI). Thus, a review on organizational performance measure related to risk suggesting that the financial and non-financial performance would serve as construct of organizational performance for the universities. Financial performance includes income generation, annual operating expenditure, cash flow impact, accountability, and securing external and international research grants. The non-financial measures include impact on international ranking, reputation, academic performance, good governance, talent management and readiness of successors of university's human resource, and impact of risks on continuity of business operation.

Organizations that implement effective risk management become successful while others not practicing this activity proved to be unsuccessful (Salman and Zain Ul-Abideen, 2010). Other studies indicated that adoption of ERM or effective implantation of risk management practices affects organizational performance (COSO, 2004, Gordon, et.al, 2009). Risk management contributes to the demonstrable achievement of objectives and improvement of performance (MS ISO 31000:2010). Thus, it can be hypothesized that in Malaysia's public autonomous universities setting, effective risk management practices could lead to organizational performance.

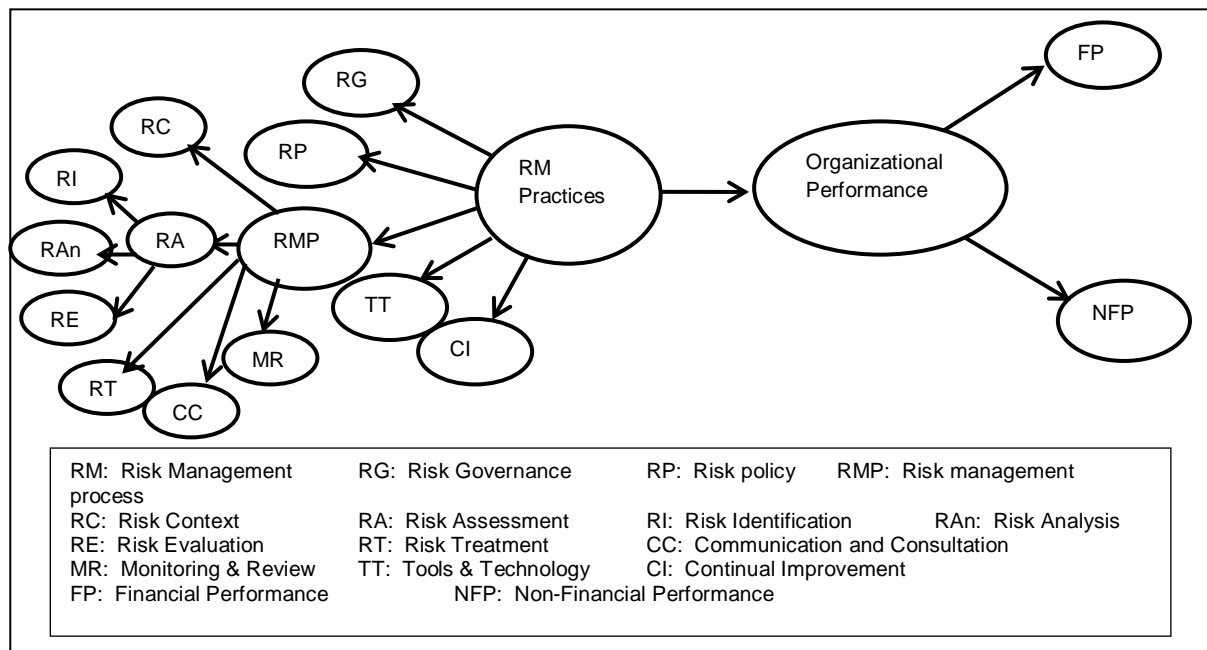
#### **2.4 Proposed Risk Management Framework and Organizational Performance**

Figure 1 illustrates the framework for risk management practices and organizational performance for the universities. It highlights:

- Risk management practices which include (i) risk governance, (ii) risk policy, (iii) risk context, Risk assessment (identification, analysis, evaluation), and risk treatment, communication and consultation and monitoring and review of risk management processes, (iv) tools and technology, and (v) continuous improvement of risk management framework;
- Measure of financial and non-financial of organizational performance in the universities; and
- The impact of the risk management practices on the organizational performance.



Figure 1: Framework of the risk management practices and organizational performance



### 3.0 Conclusion

A framework of risk management practices and organizational performance in the Malaysia’s public universities is not yet established. The common method for managing risk is relatively based on criteria specified in the UGGI, which is insufficient and lack of systematic approach to managing risk. For example, the UGGI highlighted the need to ‘set the risk parameter’, ‘understand major risk exposures’ and ‘consider the risk factors in all decisions (UGGI – para BR11, 12 and 13), but how to conduct risk management process, tools and technology used in the process, and risk treatment strategy are not properly addressed. Risk management models like MS ISO 31000:2010 and COSO are generic in nature and they are relatively applied in profit organizations. Therefore, a new framework for managing risk innovatively in the universities must be explored to help the universities pursuing their aspiration of becoming competitive higher education institutions in global education industry. Thus, this framework is expected to produce a risk management practices that will stimulates innovative idea of managing risk in higher education, specifically in the autonomous public universities setting, and offers transformative research idea in the area of risk management for non-profit organizations.

### Acknowledgements

The authors would like to thank to the Faculty of Management, ERGS research grant Vot.Q.J130000.2829.07J81 (MOHE) and UTM Johor Bahru.

## References

- [1] Ahmed, A., Kayis, B. and Amornsawadwatana, S. (2007), "A review of technicians for risk management in projects", *Benchmarking International Journal*, Vol.14 No. 1, pp. 22-36.
- [2] Association of Governing Boards of Universities and Colleges and United Educators, (2009).
- [3] AS/NZS ISO 31000:2009, Risk Management – Principles and Guidelines, Standards New Zealand
- [4] Azira Ahmad (2014). Examining Risk Behaviour and Risk Management Practices In Oil And Gas Construction Industry. Unpublished Master Thesis, UTM.
- [5] Prasanta Kumar Dey, Jason Kinch, Stephen O. Ogunlana, (2007) "Managing risk in software development projects: a case study", *Industrial Management & Data Systems*, Vol. 107 Iss: 2, pp.284 - 303
- [6] *Enterprise Risk Management—Integrated Framework, Executive Summary*, Committee of Sponsoring Organizations of the Treadway Commission, September 2004. Online at: [www.coso.org/documents/COSO\\_ERM\\_ExecutiveSummary.pdf](http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf).
- [7] Gordon, L. A., Loeb, M. P., & Tseng, C. Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, 28(4), 01-327.
- [8] Helsloot, I., & Jong, W. (2006). Risk Management in Higher Education and Research in the Netherlands. *Journal of Contingencies & Crisis Management*, 14(3), 142-159. doi: 10.1111/j.1468-5973.2006.00490.x
- [9] Kwak, Y.H., Stoddard, J. (2004). Project Risk Management: Lessons learned from software development environment. *Technovation*, 24(11), 915-920.
- [10] Kutsch, Eltnar, Browning, Tyson R., & Hall, Mark. (2014). Bridging the Risk Gap. *Research Technology Management*, 57(2), 26-32. doi: 10.5437/08956308X5702133.
- [11] Li, S.*et al.*, (2005). "Development and validation of a measurement instrument for studying SCM practices". *Journal of Operations Management*, Vol. 23(6): 618-641.
- [12] MS ISO 31000:2010, Risk management – Principle and Guideline, Department of Standard Malaysia.
- [13] Saleem, S., and Abideen, Z. A. (2010). Do effective risk management affect organizational performance, *European Journal of Business and Management* ISSN 2222-1905 (Paper)ISSN 2222-2839 (Online), Vol 3, No.3, pp. 258 – 267.
- [14] International Risk Governance Council (2005): White Paper on Risk Governance: Towards an Integrative Approach. Online version accessible at: [http://irgc.org/wp-content/uploads/2012/04/IRGC\\_WP\\_No\\_1\\_Risk\\_Governance\\_reprinted\\_version\\_3.pdf](http://irgc.org/wp-content/uploads/2012/04/IRGC_WP_No_1_Risk_Governance_reprinted_version_3.pdf)
- [15] Tufano, P. (2011), *Managing Risk in Higher Education*, Forum Future, pp. 54-58.
- [16] Ministry of Higher Education Malaysia (2011): *The National Higher Education Action Plan Phase 2 (2011 - 2015)*. Online version accessible at:
- [17] <http://www.mohe.gov.my/transformasi/fasa2/psptn2-eng.pdf>

- [18] Tchankova, L. (2002) "Risk identification – basic stage in risk management", *Environmental Management and Health*, Vol. 13 Iss: 3, pp.290 - 297
- [19] Wang, F-K., and Du, T. (2007). "Applying capability index to the supply network analysis". *Total Quality Management & Business Excellence*, Vol. 18(4), 425-434.
- [20] Wang, J. And Lin, W.(2010). A performance-oriented risk management framework for innovative R&D projects, *Technovation*, doi:10.1016/j.technovation.2010.07.003