International Journal of Theoretical and Applied Sciences **4**(1): 41-47(2012) **ISSN No. (Print) : 0975-1718**
ISSN No. (Online) : 2249-3247

Optimization of Different Objective Function in Risk Management System to Launch New Version of Product

Rajesh Shrivastava*, Shweta Singh** and G.C. Dubey***

Department of Mathematics,
**Government Science and Commerce College, Benazir, Bhopal, (M.P.)*
***Radharaman Institute of Technology and Science, Bhopal, (M.P.)*
****Government M.G.M. College, Itarsi, (M.P.)*

(Received 11 April, 2012, Accepted 12 May, 2012)

ABSTRACT : Due to technical advancement and needs of the person, the life cycle of product have been shortened. With the customer needs the functional product should be quickly improved in quality for corporate survival. In launching the development product diverse risk factors come into development of products as obstacles. Therefore the risk factors which occurs during the product development need to be managed in project planning and risk management system. Here we will study individual and integrated risk factor degree to produce NPD. Optimization of activity against risk factors can be calculated to minimize time and cost. Here a systematic frame work for risk management is proposed for handling risk degree, risk factors and occurred activities in production.

Keywords : New product development (NPD), risk degrees, SDLC (System Development Life Cycle) risk management framework, data flow diagram.

I. INTRODUCTION

Financial and economic risk analysis is a technique that enables us to determine how much risk there is in accepting or rejecting a particular project. Making risk characteristics more complete, subtler and more data rich should help decision - makers make more balanced, subtler and better - informed decisions. In fiercely competitive mark the release of new product with innovative functions and performance is a required stategy for corporate survival and required factor for having the advantage in corporate compeletion. The technique take into account possible variations in the cost and benefits that we use single best - guess numbers in an everything-goes-accordingly-to-plan analysis.

Worldwide, approximately 80% of manufacturer new product development projects fail before completion. More than half of the 20% of successful cases fail to return investment costs and become profitable. Improved equity is also a result of good NPD. Equity is traditionally discussed in terms of two polar concepts: Equity of opportunity and equity of income. The purpose of this study is to find the risk factors that may occur in each phase of a NPD project in advance and to develop a systematic risk management framework. Also the concept of equity of opportunity has much appeal if resulting differences in income distribution are due to differences in individual efforts only. The concept of equity of outcome has a lot of appeal on moral grounds but it encounters difficulties once changes in individual behaviour are brought into the picture.

The main reasons why most of the companies have failed in the development of new product are basically because the higher costs and more time have been used than expected to achieve the project goals [1] [2] [3].

The launch of new version of product undergoes a variety of risks, can affect an investment. Some common sources of risk are the following :

(*i*) *Investment Lumpiness :*

Can the product be tested gradually, or is it all or nothing ?

(*ii*) *Timing :*

What if the project is delayed? What if it takes longer than expected for the project to reach full production? Is there a best time to start the project ?

(*iii*) *Salvageability :*

How much of the investment can be recouped if this go wrong ?

(*iv*) Uncertain incremental effect :

What discount rate and inflation rates are appropriate ?

(*v*) *Volatile Preferences :*

Are the target beneficiary is needs or preferences unstable ?

The purpose of this study is to find the risk factors that may occur in each phase of NPD project in advance and to developed a systematic risk management framework. The framework can also propose the optimized responding activities against various risk factors not only to minimize the project time and cost but also to reduce the risk degrees computed in each phase and integrated risk degree entire project.

II. BACKGROUND RELATED RISK MANAGEMENT

Every individual wishes to know how 'best' to invest money to attain the maximum gain. To achieve this objective, a proper investment analysis is to be made. Dealing with risk, and income risk in particular, is not a new challenge for mankind. But new challenges are emerging, for instance, from globalization, which raises the need for managing risk in a pro-active manner to be able to grap opportunities for economic development and poverty reduction.

The previous studies related to risk management methods is NPD can be summarized as follows Savci and Kayis [4] established a risk classification system in order to identify risk factors in NPD projects. Ahmed *et al.* [5] and Dey [6] proposed the AHP method far risk analysis, and evaluated the impact of each risk factor in a project by performing pair-wise comparison. Bowles and pelaez [7] applied the fuzzy theory to assess risk factors, Choi and Ahn [8]. Risk Alalysis models and risk degree determination in new product development. Carr and Tah. [9] "A fuzzy approach to construction project risk assessment and analysis: construction project risk management system". As a risk evaluation method, the fuzzy model was used. Wu *at al.* [10] used Graphical Evaluation and Review Technique (GERT) as a model for managing risk factors during product development based on con current engineering.

Recent trends in the evolution of trade, technology, and political systems have generated great potential for improvements in welfare around the world. Mainly risk management systems have generated great potential for improvements in welfare around the world. Mainly risk management systems are still mainly intended for the development of finance, construction, R and D projects.

III. KEY CONCEPT OF THE NEW CONCEPTUAL FRAMEWORK

Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptual level. The ultimate goal is to help organization to better manage IT - related mission risk.

Key roles in Risk Management :

Ngai and Wat [11] "Fuzzy decision support system for risk analysis in e-commerce development", Ulrich and Eppinger [12] "Product Design and Development", Singh [13], "System approach to computer integrated design and manufacturing". Gives the basic idea of the Risk management responsibility. This section describes the key roles of the personnel who should support and participate in the risk management process.

(*i*) **Senior Management :** Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management.

(*ii*) **Chief lnformation Officer (CIO) :** The CIO is responsible for the agency's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.

(*iii*) **System and Information Owners :** The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. Typically the system and information owners are responsible for changes to their IT systems. Thus. they usually have to approve and sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware). The system and information owners must therefore understand their role in the risk management process and fully support this process.

(*iv*) **Business and Functional Managers :** The managers responsible for business operations and IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accompl ishment. Their involvement in the risk management process enables the achievement of proper security for the IT systems, which, if managed properly, will provide mission effectiveness with a minimal expenditure of resources.

(*v*) **ISSO :** IT security program managers and computer security officers are responsible for their organizations' security programs, including risk management. Therefore, they playa leading role in introducing an appropriate, structured methodology to help -identify, evaluate, and .minimize risks to the IT systems that support their organizations' missions'. ISSOs also act as major consultants in support of senior management to ensure that this activity takes place on an ongoing basis.

(*vi*) **IT Security Practitioners :** IT security practitioners (*e.g.*, network, system, application, and database administrators; computer specialists; security analysts; security consultants) are responsible for proper implementation of security requirements in their IT systems. As changes occur in the existing IT system environment (*e.g.*, expansion in network connectivity, changes to the existing infrastructure and organizational policies, introduction of new technologies), the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems.

(*vii*) Security Awareness Trainers (Security/Subject Matter Professionals) : The organization's personnel are the users of the IT systems. Use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training. Therefore, the IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.

Risk factor and Risk Degrees :

A risk factor is defined as an event that can occur and may negatively affect total cost, required time, and the quality of new product in a new product development project.

For example : The Table 1 shows the risk factors examined, collected, and categorized under this definition.

Table 1 : Classification of risk factors by phase and functions [n].

Category [b]	*Risk of Factor*	*Phase* [c]						*Function*			
		0	*1*	*2*	*3*	*4*	*5*	*Project Mgt.*	*Marke -ting*	*De- sign*	*Mfg.*
R	Critical resources may not be available when required	0	0	0	0	0	0	0	0	0	0
P	Failure to effectively mix internal and external expertise	0	0	0	0	0	0	0	0	0	0
T	Inadequate user documentation	0	0	0	0	0	0	0	0	0	0
T	Incorrect system requirements	0	0	0	0	0	0	0	0	0	0
P/S	Lack of integration	0	0	0	0	0	0	0	0	0	0
P/S	Lack of proper management control structure	0	0	0	0	0	0	0	0	0	0
P	Lack of senior management support	0	0	0	0	0	0	0	0	0	0
R	Litigation in protecting intellectual property	0	0	0	0	0	0	0	0	0	0
0	Low interest rate	0	0	0	0	0	0	0	0	0	0
0	Sudden change of foreign exchange rate	0	0	0	0	0	0	0	0	0	0
P	Team members not familiar with the task(s) being automated	0	0	0	0	0	0	0	0	0	0
0	Change in organizational management during the project		0	0	0	0	0	0			
P	Lack of available project management skill	0	0	0	0	0	0	0			
P/S	Project objectives are poorly defined.	0	0	0	0	0	0	0			
P/S	Unplanned work that must be accommodated	0	0		0	0	0	0			
T	Cutting edge, demanding technical effort	0	0	0	0	0	0		0	0	0
T	Inappropriate user interface	0	0	0	0	0	0		0	0	
P	Lack of business analysts with business and technology Knowledge	0	0	0	0	0	0		0		
T	Inadequate specification		0	0	0	0	0		0	0	0
T	Insufficient or incorrect design information		0	0	0	0	0			0	0

(*a*) These are some examples of more than 200 risk factors. More risk factors would be collected and classified by functions and phases in further research.

(*b*) Risk factor related to people (P), technology (T), resources (R), process/planning/scheduling (P/S), and others (O).

(*c*) The phases mean the sequential steps in NPD such as planning(0), concept development(1), system-level design (2), detail design (3), testing and refinement (4), and production ramp-up (5).

Risk Degree :

Risk degree denoting the impacts of risk factors is show in equation (1).

$$R = P \times I \quad \text{... (1)}$$

where R = Risk degree

P = Probability of risk occurrence (0 ~ 1)

I = Risk factor impact (0 ~ 1)

In order to calculate the risk degree of an entire project, risk factors that may occur in the project should be identified as many as possible and (1) should be used to calculate individual risk degrees.

Detailed Methodologies :

1. *Risk Assessment*

Risk assessment is the first process in the risk management methodology. Organization use risk assessment to determine the extent to the potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during risk mitigation process.

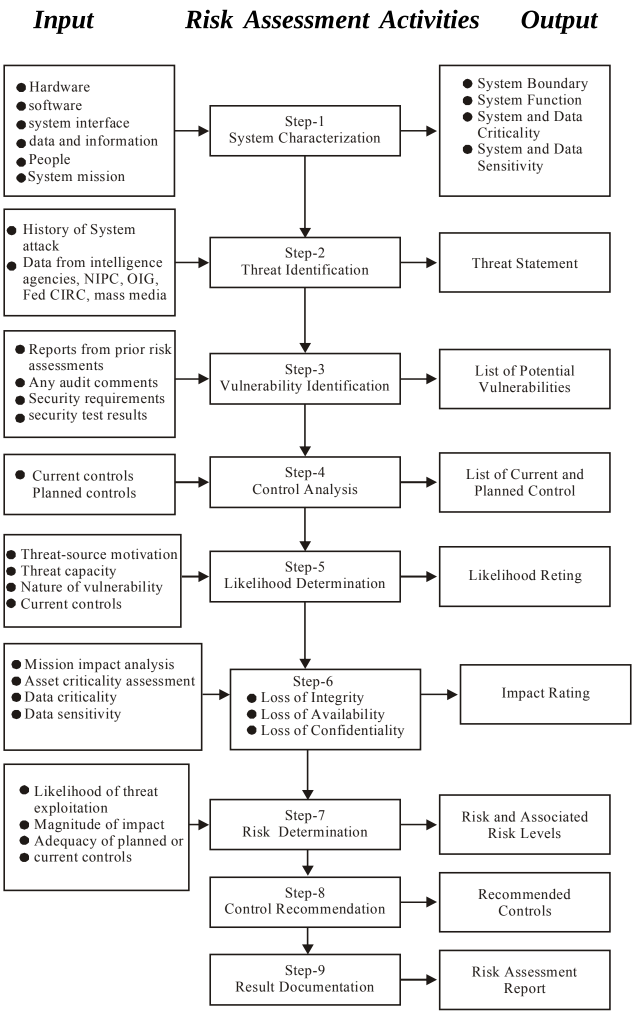

Fig. 1. Risk assessment methodology flow chart.

2. *Risk Mitigation*

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk - reducing controls recommended from assessment process, which is describe in risk mitigation methodology flow chart.

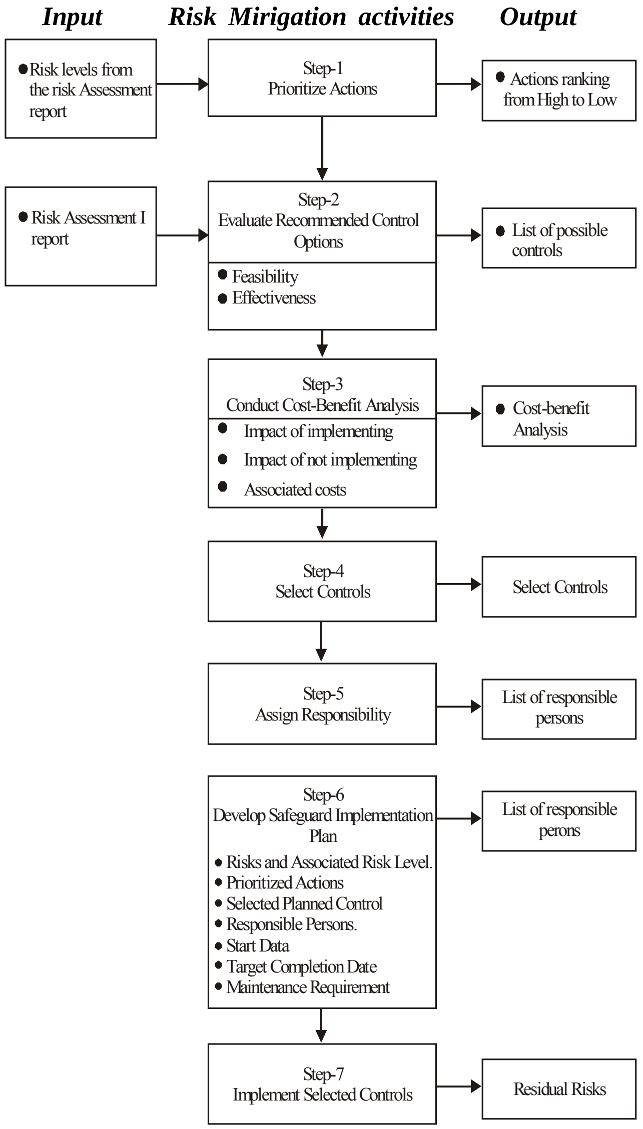
Input
Risk Mirigation activities
Output
● Risk levels from the risk Assessment report
Step-1
Prioritize Actions
● Actions ranking from High to Low
● Risk Assessment I report
Step-2
Evaluate Recommended Control Options
● Feasibility
● Effectiveness
● List of possible controls
Step-3
Conduct Cost-Benefit Analysis
● Impact of implementing
● Impact of not implementing
● Associated costs
● Cost-benefit Analysis
Step-4
Select Controls
Select Controls
Step-5
Assign Responsibility
List of responsible persons
Step-6
Develop Safeguard Implementation Plan
• Risks and Associated Risk Level.
• Prioritized Actions
• Selected Planned Control
• Responsible Persons.
• Start Data
• Target Completion Date
• Maintenance Requirement
List of responsible perons
Step-7
Implement Selected Controls
Residual Risks

Fig. 2. Risk mitigation methodology flowchart.

As the elimination of all risk is usually impractical, it is the responsibility of senior management and functional and business managers to use the least - cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level.

The risk migration chart in Fig. 4 addressess these questions. Appropriate points for implementation of control action are indicated in this figure by the word YES.

This strategy is further articulated in the following rules of thumb, which provide guidance on actions to mitigate risks from intentional human threats:

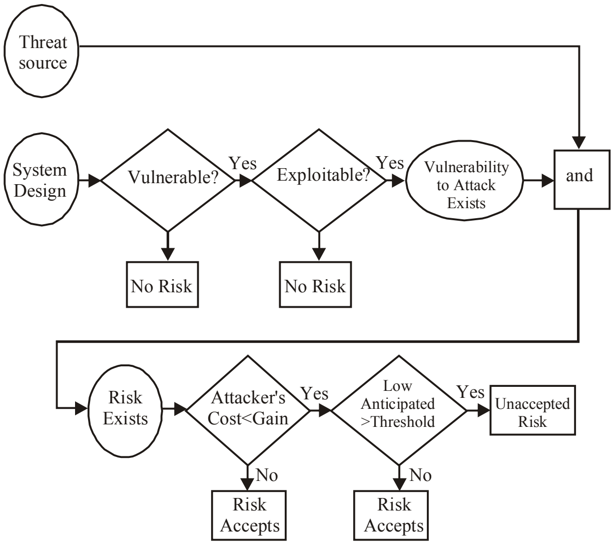

Fig. 3. Risk mitigation action points.

(*i*) When vulnerability (or flaw, weakness) exists implement assurance techniques to reduce the likelihood of a vulnerability's being exercised.

(*ii*) When a vulnerability can be exercised apply layered protections, architectural designs, and administrative controls to minimize the risk of or prevent this occurrence.

(*iii*) When the attacker's cost is less than the potential gain apply protections to decrease an attacker's motivation by increasing the attacker's cost (*e.g.*, use of system controls such as limiting what a system user can access and do can significantly reduce an attacker's gain).

(*iv*) When loss is too great apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.

3. *Risk impact depending the difficulty level project*

The Importance of each risk factor is calculated by performing AHP analysis to be done by experts in the field. Even though experts experience and knowledge can be quantified by the AHP analysis, this output value still implies the subjectivity and ambiguity of experts

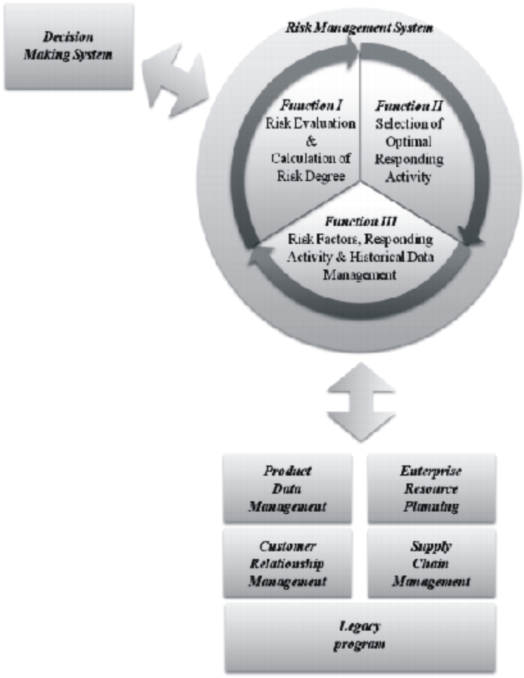
Decision Making System
Risk Management System
Function I Risk Evaluation & Calculation of Risk Degree
Function II Selection of Optimal Responding Activity
Function III Risk Factors, Responding Activity & Historical Data Management
Product Data Management
Enterprise Resource Planning
Customer Relationship Management
Supply Chain Management
Legacy program

Fig. 4. Risk management framework and network architecture.

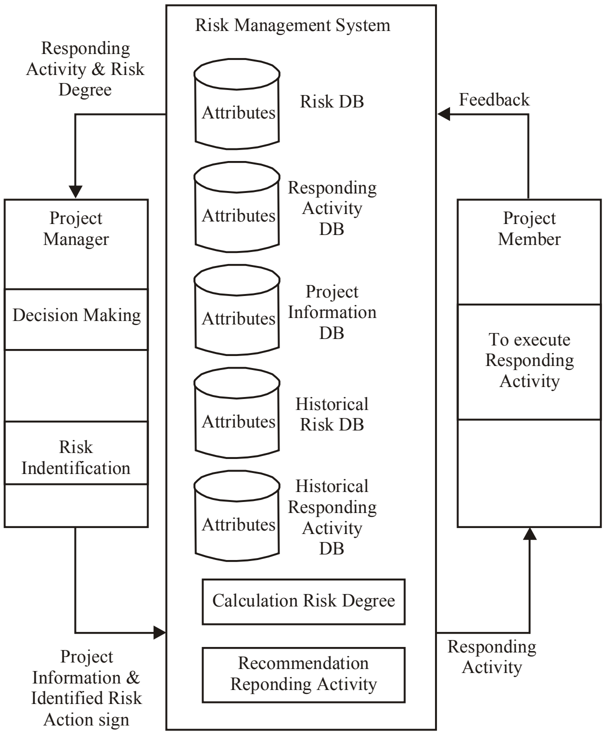

Fig. 5. Risk management system framework.

4. *Risk Determination at various Risk - level matrix*

To measure risk, a risk scale and a risk - level matrix must be developed. The table below shows how the overall risk rating be determined based on inputs from the threat likelihood and threat impact categories. The matrix below is a 3 × 3 matrix of threat likehood (high, medium, low) and threat impact (high, medium, low). The sample matrix in table below shows the overall risk level of high, medium, low are derived.

Table 2: Risk-level matrix.

Threat	*Impact*		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low 10 × 1.0 = 10	Medium 50 × 1.0 = 50	High 100 × 1.0 = 100
Medium	Low 10 × 0.5 = 5	Medium 50 × 0.5 = 25	High 100 × 0.5 = 50
Low (0.1)	Low 10 × 0.1 =1	Medium 50 × 0.1 = 5	High 100 × 0.1 = 10

Risk Scale : High (> 50 to 100); Medium (> 10 to 50); Low (1 to 10)[8]

Table 3: Risk Scale and Necessary Actions.

Risk Level	*Risk Description and Necessary Actions*
High	If an observation or finding is evaluated as a high risk, there is a High strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	Low If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

5. *Probability Distribution in Risk Management*

To do risk analysis, we need to know the range of values each variable can take (minimum to maximum) and the probability distribution of values in that range.

Example : If the price of a barrel of oil is between $12 and $32 and the probability of any value in that range is described by a uniform probability distribution, then the computer has all the information is needs to sample values of the price of oil to use in iteration of benefit - cost model. Identifying the probability distribution within that range is more difficult. Suppose se have monthly oil - price data for the past 10 years. The first step in identifying the probability distribution for oil prices is to group raw data.

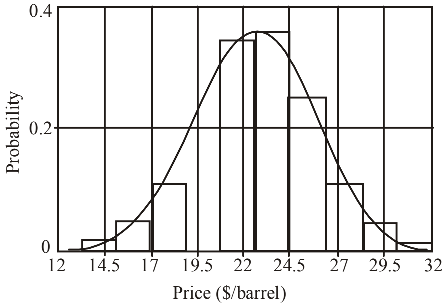

Fig. 6. A Normal asure filted to a frequency histogram.

6. *Integrated Risk degree in Risk Management*

Minimizing negative impact on an organization and need for sound basis in decision making are the fundamental effective risk management must be totally integrated into the SDLC (System Development Life Cycle).

In order to calculate the integrated risk degree, to synchronize risk degree for an entire project, the risk degree of each development phase is integrated first [14]. The harmonic mean of individual risk degrees for any and all risk factors that may occur in each phase is calculated by using (2). The reason for using harmonic mean is that more that are risk factor may occur simultaneously in a step.

$$R_p = \frac{n}{\sum_{i=1}^{n} \frac{1}{r_i}} \qquad \text{... (2)}$$

After the harmonic mean is obtained in each phase, the integrated risk degree of the entire project is calculated by, arithmetic mean as show in (3).

$$R_{ALL} = \frac{\sum_{p=0}^{5} R_p}{6} \qquad \text{... (3)}$$

where p is the development phase

II. CONCLUSION

The proposed new conceptual or version of product using Risk Management System, framework as well as their implementation, the true value of any new concept lies in its ability to help better understand and map reality and propose and implement better policies. Here the verdict is still out, but there is cause for optimism.

In addition, their application are limited to finance, construction, R and D project management etc. thus, those who try to handle those risk, analysis models, especially for NPD, may have difficulties in setting the scope of risk factors and in determing responding activities at all the project planning stage.

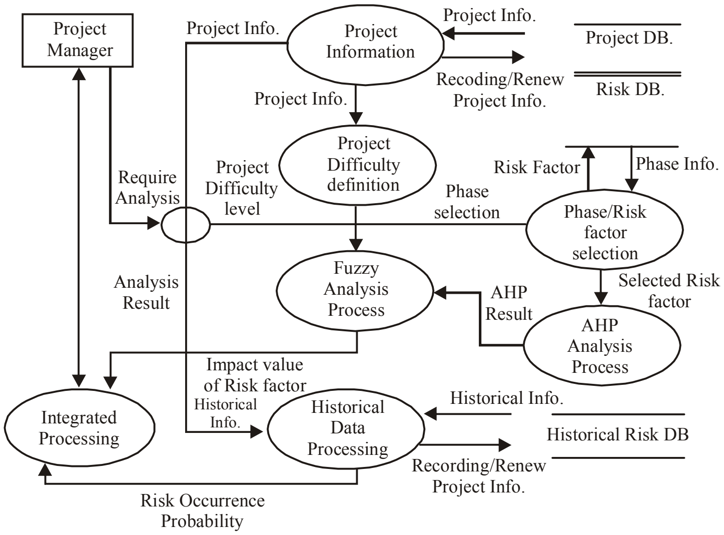

Fig. 7. Data flow diagram for integrated risk degree.

REFERENCES

[1] Coppendale, J., "Manage risk in product and process development and avoid unpleasant surprises", *Journal of Engineering Management*, Vol. **5**, pp. 33-38, (1995).

[2] Cooper, L.P., "A research agenda to reduce risk in new product development through knowledge management: a practitioner perspective", *Journal of Engineering and Technology Management*, (2003).

[3] Ahn, J.O., Jeung, H.S., Kim, J.S. and Choi, H.G., "A framework for managing risks on concurrent engineering basis", *Proceedings of the IEEE International Conference on Management of Innovation and Technology*, (2008).

[4] Savci, S. and Kayis, B., "Knowledge elicitation for risk mapping in concurrent engineering projects", *International Journal of Production Research*, **44**, 9, pp. 1739-1755(2006).

[5] Ahmed, A., Kusumo, R., Savci, S., Kayis, B., Zhou, M. and Khoo, Y.B., "Application of Analytical Hierarchy Process and Bayesian Belief Networks for Risk Analysis", *Complexity International*, **12**(2005).

[6] Dey, P.K., "Project Risk Management: A Combined Analytic Hierarchy Process and Decision Tree Approach", *Cost Engineering*, **44**(2002).

[7] Bowles, J.B. and Pelaez, C.E., "Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis", *Reliability Engineering and System Safety*, **50**, pp. 203-213(1995).

[8] Choi, H.G. and Ahn, J.O., "Risk analysis models and risk degree determination in new product development: A case study", *Journal of Engineering and Technology Management*, pp. 110-114(2010).

[9] Carr, V. and Tah, H.H.M., "A fuzzy approach to construction project risk assessment and analysis: construction project risk management system", *Advanced in Engineering Software*, Vol. **32**, (2001).

[10] Wu, D.D., Kefan, X., Gang, C. and Ping, G., "A Risk Analysis Model in Concurrent Engineering Product Development", *Risk Analysis*, Vol. **30**, No. 9, (2010).

[11] Ngai, E.W.T. and Wat, F.K.T., "Fuzzy decision support system for risk analysis in e-commerce development", *Decision Support Systems*, **40**, pp. 235-255, (2005).

[12] Ulrich, K.T. and Eppinger, S.D., "Product Design and Development", McGraw-Hill, Chap. 2, (2004).

[13] Singh, N., "System approach to computer-integrated design and manufacturing", John Wiley and Sons, Chap. 4. (1996).

[14] Choi, D.W., Kim, J.S., and Choi, H.G., "Determination of Integrated Risk Degrees in Product Development Project", *Proceedings of the World Congress on Engineering and Computer Science*, Vol. **II**, (2009).