Estimating operational risk indices for software services outsourcing industry: a case

J. Dasgupta

ITM – BIT Collaborative Research Program,
Patni Computer Systems Limited,
SEEPZ, Andheri (East),
Mumbai 400 096, India
Email: jyotidasgupta@yahoo.co.in

R.P. Mohanty*

ITM Group of Institutions,
B.S.E.L. Tech Park, 704-712,
Sector 30 A, Vashi,
Navi Mumbai 400 705, India
Email: rpmohanty@gmail.com
*Corresponding author

Abstract: Software Services Outsourcing (SSO) industry has grown rapidly in the last few decades in undertaking software projects. Projects are grouped with several other projects according to some similarity, for example same customer, same domain, same geography, or some other factor(s). When an SSO enterprise undertakes concurrent execution of multiple projects characterised by size, complexity, resource requirements, etc. in multiple locations, it is necessary to estimate 'generic risk factors'. Although generic risk factors are used in medical/actuarial science, so far they have not been applied in SSO industry and therefore have not been mandated in the existing IT-related standards; which currently focus on project-specific risk factors. In this paper, we demonstrate the use of generic risk factors by developing a computational and workflow system framework. Such a framework may be used to upgrade existing international standards on project risk management.

Keywords: services; standards; software project risk management; software project outsourcing; operational risk indices; project-specific risk indices; generic risk indices; enterprise risk index; computational and workflow system framework.

Reference to this paper should be made as follows: Dasgupta, J. and Mohanty, R.P. (2010) 'Estimating operational risk indices for software services outsourcing industry: a case', *Int. J. Services and Standards*, Vol. 6, No. 1, pp.43–61.

Biographical notes: J. Dasgupta is the Head of Quality Department at Patni Computer Systems Limited, one of the largest software services companies in India. He received Bachelors degree in Electronics and Communication Engineering from the University of Roorkee, a Masters degree in Software Systems from the Birla Institute of Technology and Science, Pilani, and is currently pursuing doctoral research through the collaborative research

programme between ITM, Navi Mumbai, and Birla Institute of Technology, Ranchi. He has over three decades of work experience in the field of software, and software project management across the globe.

R.P. Mohanty is the Chair Professor and Dean with ITM Group of Institutions located in various metro cities of India. He has 32 years of academic experiences in institutes of national (India) importance and in some foreign universities. He has ten years of industry experience in top management positions. He advises academic institutions and industries, supervises research scholars and undertakes sponsored research projects. He has published more than 250 papers in scholarly peer reviewed international journals and has also authored eight books. Many professional institutions, both in India and abroad, have honoured him.

1 Introduction

IT services can be obtained from in-house IT departments, or from a vendor. Procuring IT services from vendors is termed outsourcing. Software Services Outsourcing (SSO) is a common practice any where in the world (Kakumanu and Portanova, 2006). By the beginning of this century, over three quarters of large firms were engaged in long-term SSO contracts. Primary drivers for outsourcing are desire to reduce costs or increase profitability, desire to focus on core competency, access to special expertise, speeded up delivery, relieving resource constraints and many others (Davies, 2004). Estimates vary but most agree that the global outsourcing market is pegged upwards of a trillion US dollars. According to one study, 57% of this market was serviced by the USA, 4% by India, 3% by China, Philippines and SE Asia, and 36% by other countries (Brown and Wilson, 2007). Another study concluded that the worldwide IT services spending aggregated nearly USD 1.7 trillion, and computed a growth of 7.3% over the previous year. Two major components of this market were found to be:

- Software Services Outsourcing: Software and other services including Business Process Outsourcing (BPO) at USD 1.2 trillion – over 71% of the total spend in 2007.
- Hardware spends, at USD 478 billion, accounted for over 28% of the total worldwide IT services spending in 2007 (NASSCOM, 2008).

In this paper, we first review the globally recognised standards that are in use in SSO industry, as well as the existing literature on project risk management. We then introduce the concept of project-specific and generic software project risk factors. To understand the concept of generic risk factors, we cite two research studies. Koong et al. (2008) analysed occurrences of internet fraud in the USA between 2002 and 2006, and found that there were correlations between factors such as places with more people, more transactions, digital divide and specific regions with the trend in internet frauds. Kasiri and Sharda (2008) demonstrated that time wasted through frequent e-mail checking and response is dependent upon generic 'job context' factors such as incoming e-mail frequency, interruption cost and time available to spend on e-mails. Koong et al. (2008) had recommended that these generic factors can be used by services and standards experts and enforcement agencies. Generic software project risk factors can also be similarly used by services and standards experts, and SSO management.

Unlike project-specific risk factor based indices, generic risk indices can be aggregated to give higher levels of grouping, for example Group Risk Index (GRI), or Enterprise Risk Index (ERI). Utility of such level wise and aggregated analysis in the information systems service quality had been reported by Miller et al. (2008).

We also develop computational system framework and workflow that exploit both generic and specific project risk factors. We have deployed and validated this framework and workflow in a 'Mid-sized Software Company (MISCO)' for more than two years. Results and significant findings from MISCO have been presented. The principal objective is to take a comprehensive look at some of the important concepts in risk identification and measurement that apply to SSO industry from vendors' perspective, and also to propose a set of Operational Risk Indices based on generic and project-specific risk factors. We propose that these can become part of IT and other related service standards. The computational and workflow system framework developed and validated in this paper can also be incorporated in relevant international standards. Such upgrades in standards should facilitate SSO management to divert multiple scarce resources to projects in greater need compared to some other projects.

2 Risk management for software services outsourcing industry

SSO is a mega growth industry. This industry has seen scores of young technocrats build multi-million dollar enterprises. IT industry business models are very sophisticated, and have given extra momentum and impetus to innovative financing models including venture capital and equity markets, both private and public. Although most IT companies begin as 'start ups' with shares held by only early stage financiers, they soon become answerable to millions of shareholders after going public. Revenue predictability and preserving shareholder value become important to such companies.

SSO companies have witnessed higher than average revenue, and margin growth over the last several decades. Increasingly, however, the growth rates are under threat. Past events such as the dotcom bust, terrorist strikes or recent event like meltdown in global financial markets have meant cautious capital expenditure spends, and postponing technology upgradation plans.

Consequently, ability of SSO industry to face adversities must increase to maintain sustainable global competitiveness. Other more traditional industries such as Finance or Manufacturing have been using sophisticated risk management techniques for decades; and have benefited immensely. Indeed, it is impossible to visualise those industries without risk management systems. Although SSO industry lagged initially, many companies have started implementing risk management systems (Dasgupta and Mohanty, 2009), enterprise risk management systems (Beasley et al., 2004) and special risk audits in recent past (Brandas, 2010).

2.1 International standards used in SSO industry

Various globally recognised and accepted standards that are in use in SSO industry are presented in Table 1.

Table 1 Standards and frameworks commonly used in SSO industry

Quality Management	*Organisation Performance*	*Governance*	*IT Management*	*Project Management*	*Security Management*	*IT Investment Management*	*Others*
TQM	Balanced Scorecard	AS 8015	ITIL	MSP	ISO 27001/BS 17799	North Carolina Framework for Managing IT Investments	PSP
						Government Accountability Office	
ISO 9001	Six Sigma	COBIT	eTOM	PRINCE2	BS 25999	IT Investment Management Framework (ITIM)	TSP
				IPMA Competence Baseline	Cert Resiliency Management	Val IT	P-CMM
TickIT/ISO 12207	MBQNA	M_o_R	ASL				
CMMI		ISO 38500	BiSL	PMBoK			
ISO 20000			ISPL				
COPC 2000							
eSCM-SP							

We examined all these standards and it could be seen that none of these standards incorporate generic risk factors.

2.2 Managing SSO risks

SSO units the world over are implementing risk management systems. Focus of research earlier was on software projects from the internal IT department's perspective, subsequent researchers found substantial differences in the way risk is perceived and therefore, should be managed by vendors. Important differences are as follows:

- SSO vendors execute large number of projects. SSO vendors would typically execute several hundred projects at any time. In-house IT projects are usually less in number comparatively. SSO vendors have the need to aggregate risks. This is similar to say Insurance industry, where risks are computed at an individual's level, as well aggregated as a group.
- SSO vendors have a need to mitigate risks at project level, as well as at aggregate level.
- SSO vendors have the need to link risk levels with the financial forecasting process.

A SSO vendor is a business entity and therefore, effective analysis of financial performance is of much importance to it. Assessing risks and incorporating the same in the final decision is an integral part of financial analysis (Chandra, 2003). Risk management techniques are used in most major enterprises and considerable knowledge exists on how to effectively assess and mitigate risks.

2.3 Risk classification

Although several risk classification schemes exist (Lam, 2003; COSO, 2004; Fight, 2004; Escobar and Seco, 2008), simple classifications that are sufficient for most purposes, and are often used by risk professionals, recognise three major types of risks:

- *Market Risk*: Prices will move in a way that has negative consequences for the enterprise.
- *Credit Risk*: A customer, counter party, or supplier will fail to meet its obligations.
- *Operational Risk*: People, processes or systems will fail, or an external event (e.g. earthquake, fire, etc.) will negatively impact the enterprise.

In general, risk managers would consider market risk and credit risk as financial risk, and group all other risks as part of operational risk (Lam, 2003).

In this paper, the focus is on operational risks for a SSO. SSO companies can use these Operational Risk Indices to decide which projects have more pressing needs to receive additional resources in multiple resources constrained situations, and as a forewarning tool to initiate mitigating actions on time.

2.4 Typical services provided by SSO industry

Software projects undertaken by most SSO companies can be classified into following categories according to the nature of services provided:

A *Business Transformation and Consultancy Services*.

B *Application*: These are software used by client organisations that are custom designed for in-house use by the clients themselves and not available for others.

- Development: Developing and implementing new applications.
- Maintenance: Enhancements, modifications and bug fixing of in-house applications.
- Re-engineering: Making application systems work with or without additional features on a new technology or platform.
- Localisation/Globalisation: Making the software serve different geographies and languages.

C *Software Products*: These are developed by software product companies, for use by their customers. These are also referred to as 'packages'.

- Development: Developing new or next generation products.
- Sustenance: Similar to application maintenance, but usually tasked with maintaining several past versions through out the life cycle of the software product.
- Re-engineering: Making products work with or without additional features on a new technology or platform.
- Localisation/Globalisation: Enabling products to serve different geographies and languages.

D *Package Implementation*: Software products such as ERP, BI Tools, etc. require extensive customisation for client-specific purposes. This work is referred to as package implementation.

E *Testing*: A major source of revenues, these projects require extensive manual or automated testing of software applications or products.

F *Production Support*: These projects monitor and fix applications in use (often referred to systems in production) such as an online credit processing system, or HR management system etc. on 24 × 7 basis. Often involves minor modifications or bug fixes as well.

G *Engineering and Hardware Design Services*: Offer services such as digitisation, CAD/CAM, PCB design, VLSI design, etc.

H *Business Process Outsourcing*: Data processing and call handling services for industries such as financial services, airlines, hospitality, etc.

Many SSO projects are undertaken using coordinators and analysts at client locations (called onsite) with significant portion of software work done at company owned development centres and are referred to as onsite-offshore projects.

Most SSO projects are usually billed on the following basis, with variations such as per transaction, or profit sharing, etc.

A Time and Material (T&M) billing model is used when the scope of the project cannot be defined precisely, or for repetitive maintenance or production support type work that go on for years. Services are charged on per person hour or person day basis.

B Fixed Price (FP) projects are used when the scope can be defined with reasonable precision and efforts/schedules estimated in advance.

2.5 Software project risk factors

Dictionary definition of Risk (Oxford, 2005) is 'the possibility of something bad happening in future; a situation that could be dangerous or have a bad result; any business venture has an element of risk'. The major ingredient of risk is uncertainty. If the consequences of an action or decision depend on the possible occurrence of other events, then we term such actions or decisions as 'risky', if we cannot tell in advance whether those events will happen or will not happen (Copas, 1999).

Researchers in the area of software risk management have been very active. Many give credit to Barry Boehm and Tom Demarco for laying the foundation of Software Risk management (Boehm, 1989; Boehm and Demarco, 1997) although they themselves give credit to Michelangelo for using risk management techniques in 1547 while raising the dome of St. Peters. They also call software development the 'ultimate risky business'.

One of the initial attempts to identify risk factors in software projects was made by Henri Barki, Suzanne Rivard and Jean Talbot (Barki et al., 1993). They identified 24 risk factors after a survey of 120 software projects. These factors were revalidated by Jiang et al. (2002) over 152 software projects, and six factors were found through Exploratory Factor Analysis. Several researchers have provided further insight into risks found in in-house or outsourced software projects (Mulcahy, 2003; Ethiraj et al., 2005; Cleary, 2008; Gefen et al., 2008). Of particular interest is the work done by Hazel Taylor (Taylor, 2007). She has pointed out that while many risk factors for IT projects in general have been identified in the literature; little thought have been given to the risk factors that are of higher concern for managers of vendor driven (or outsourced) projects. She has identified top risks in 'ERP implementation' type outsourced projects in Hong Kong.

Additional software project risks have been identified by international standards such as the International Standards Organization (www.iso.org) or the Integrated Capability Maturity Model CMMI® for software services from the Software Engineering Institute, Carnegie Mellon University (SEI, 2009).

We have consolidated the major factors emerging from the above body of knowledge into ten major categories. The factor categories and their explanations are given in Table 2.

Table 2 Ten major software project risk factors

Risk Category			*Explanation*
1	Requirements Risk	1	Inadequate or wrong understanding of project requirements
		2	Lack of communication with actual users of the system
		3	Inadequate change control mechanism for managing changes in requirement
		4	Unclear boundary or project scope
2	Solution Risk	1	Infeasible design
		2	New and unproven technology chosen for the project
		3	Target hardware platform is not ready or has problems
		4	3rd Party Solution related issues
3	Project Management Risk	1	Wrong effort and schedule estimates
		2	Inadequate project staffing and skills
		3	Supplier or Subcontractor related issues
		4	Not using sound project management techniques
		5	Issues with organisational change management post project implementation
		6	Size or complexity of project is very high causing problems in managing project
4	Project Staffing Risk	1	Inadequate project staffing or technical skills
		2	Inadequate business domain or client knowledge within project team
		3	High attrition, or new project team members
		4	Team morale issues
5	Project Infrastructure Risk	1	Lack of necessary development, testing or production platforms including hardware, software or network resources
		2	Unsatisfactory or uncomfortable work environment and physical support systems such as food or commuting facilities for project teams
		3	Lack of access to knowledge resources such as experts, reusable components, library, books etc.
6	Relationship Risk	1	Relationship within and between project team members
		2	Relationship with and support from users and customers
		3	Relationship with vendors and subcontractors
7	Location Risk	1	Project is at an unfamiliar location with support or physical security issues
		2	Project is spread over multiple locations, making project management difficult
8	Commercial Risk	1	Strict or unrealistic penalty clauses related to project service level agreements (SLA), performance such as speed, or schedules
		2	Cost or funding issues
		3	Intellectual Property (IP) or Litigation related issues
9	Information Security Risk	1	Failure to protect confidentiality, integrity and availability (CIA) of project information assets
		2	Malicious attack on project infrastructure through spams, virus etc.
		3	Intellectual Property (IP) leakage or Litigation related issues
10	Business Continuity and Disaster Recovery (BCP/ DRP) Risk	1	Disruptions to the continuity of operations caused by an external event such as terrorist strike, political unrest, etc.
		2	Unanticipated infrastructure failure caused by earthquake, fire, flood, etc.

3 Measuring software risk

The gold standard for decision-making is Expected Utility Theory – the optimal decision is one that maximises expected utility, essentially the product of the probability of the adverse event and the utility (negative loss), which will result if that event occurs. It is well documented that in practice people's decision-making strategies do not accord at all closely to this normative ideal, but nonetheless the decisions we make will still be strongly influenced by perceived levels of risk (Copas, 1999).

Boehm (1989) proposed an approach, which is in agreement with the Expected Utility Theory, and defined software risk exposure (RE) as:

$$\mathrm{RE} = \mathrm{Prob}\,(\mathrm{UO}) * \mathrm{Loss}\,(\mathrm{UO}) \tag{1}$$

where Prob (UO) is the probability of an unsatisfactory outcome and Loss (UO) is the loss to the parties affected if the outcome is unsatisfactory.

Software practitioners adopted Boehm's approach, and several risk indices were soon devised based on that approach. In situations where calculating probability and impact were relatively easy, this technique was found to be very suitable (Leung, 1995).

In cases where several unsatisfactory outcomes are possible with probabilities Prob (UO_i), each with losses Loss (UO_i) the total Risk Exposure can be computed as

$$\mathrm{RE} = \sum_{i=1}^{n} \mathrm{Probability}\,(\mathrm{UO}_i) \times \mathrm{Loss}\,(\mathrm{UO}_i) \tag{2}$$

For most software projects, calculating Prob (UO) was found to be difficult. This is an experience shared by many practitioners, but it continues to be widely used (Mulcahy, 2003). To overcome difficulties in assessing probabilities of adverse events, a new method was proposed (Barki et al., 1993). The alternative method proposes that:

$$\begin{aligned}\text{Software development risk} = {} & (\text{project uncertainty}) * \\ & (\text{magnitude of potential loss due to project failure})\end{aligned} \tag{3}$$

This approach differs in two major respects. First, it refers to uncertainty instead of probability, and second, it refers to only one unsatisfactory outcome, i.e. project failure instead of several unsatisfactory outcomes.

A comparison can be drawn between Barki's proposal and the risk indices used in medical studies. For example, if a correlation is found to exist between smoking or chewing tobacco with prevalence of cancer, chewing or not chewing tobacco can be used to conclude a risky behaviour. If the person also smokes, it can be said that the behaviour is even more risky. Therefore, a person who smokes and chews tobacco can be said to have a higher risk index (and therefore possibility of getting cancer) than a person who does neither or does either.

As software projects have intervening conditions, i.e. intervention by management (Kutsch, 2008), it is often enough to identify projects exhibiting higher risk index compared to other projects, to determine which projects are in need of management attention in precedence over the others. This is similar to deciding which patients require medical attention more urgently in a wartime field hospital.

4 A computational and workflow system framework towards project risk measurement

There are uncertainties associated with every software project. Some projects have more uncertainties than others. For example, a project may have been bid in fixed price (FP) mode due to competitive reasons but the requirements may not have been understood fully. Or a key project member may have moved to another project and whether complete knowledge had been transferred to another member is not known. Project uncertainties fluctuate over time, going up when adverse events introduce uncertainties into the project, and going down when the uncertainties are reduced. Higher uncertainty denotes more risk that a project would not meet project objectives. In the absence of an instrument to assess these uncertainties with reasonable accuracy, uniformity or reliability – management may be forced to take ad-hoc decisions, and resources may not get assigned to the projects in most distress. Management needs to know about risky projects for forewarning as well. Accurate information about risky project allows management to inform stakeholders including customers in advance, allowing mitigation actions on time.

4.1 Project risks and risk factors

Project risks are the chances of a project not meeting project objectives. Project objectives may be low variance of actual efforts from estimated efforts, delivering on schedule, meeting financial contribution goals, good quality, high customer satisfaction, etc.

Most SSO management would define project objective as meeting financial contribution targets. Shortcomings in other areas such as quality (bad quality leads to re-work), effort or schedule variance (more effort than previously estimated impacts project's profitability), or customer dissatisfaction (if quality, costs and schedules are met; rarely customers have reasons to be dissatisfied) should impact the projects financial contribution. We term inability to meet financial contribution as Margin Loss.

$$\text{Margin Loss} = \text{Actual Margin}(\%) - \text{Expected Margin}(\%) \tag{4}$$

4.2 Project-Specific Risk Exposure (PSRE)

Method to compute PSRE is shown in the top panel of Figure 1, in the 'project specific risk assessment' part. To compute project risk exposure due to specific and unique situations, equation (2) has been adapted as:

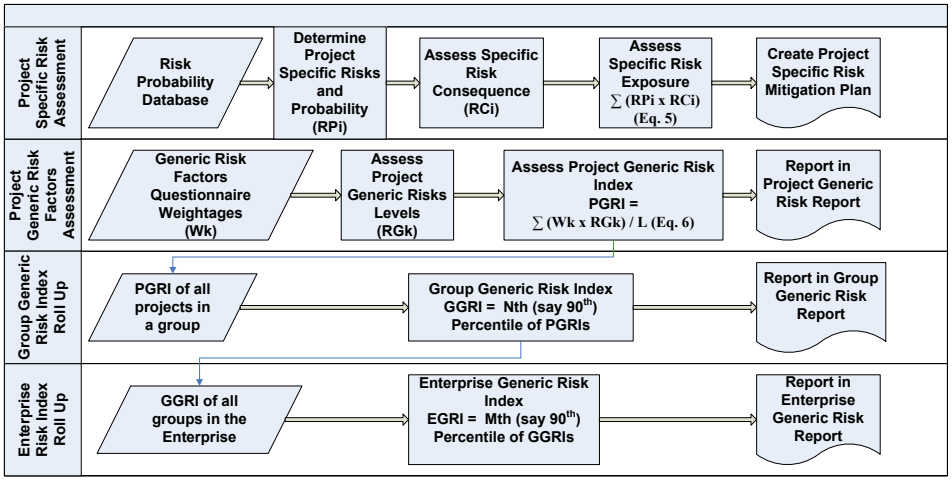
$$\text{PSRE} = \sum_{i=1}^{n} \text{RP}_i \times \text{RC}_i \tag{5}$$

where PSRE = Project Specific (or Unique) Risk Exposure

RP_i = Risk Probability or probability of the ith risk event occurring

RC_i = Risk Consequence or financial loss that may be caused if the ith risk event occurs

Figure 1 Project-specific risk exposure and generic project risk indices (see online version for colours)



PSRE is used to initiate project specific risk mitigation plans. These plans are directed at prevention of project-specific risk events occurrence. To give an example, let as assume that a particular project's manager has identified the following risk events, occurrence probabilities and consequences:

Risk Event 1: The data link line connecting the server and client machines has gone down for 32 hours at an average every year for the previous three years. Each lost hour signifies a project billing loss of USD 4800.

Risk Event 2: The project has a Service Level Agreement (SLA) that high priority bugs would be resolved in one working day. In the same previous three years, this SLA has been breached at an average seven times in a year. Each SLA breach carries a financial penalty of USD 3000.

PSRE of the project is computed as

$$32 \times 4800 + 7 \times 3000 = \text{USD } 174,600.$$

This project can reduce the PSRE by getting a backup link in place, and through reduction in SLA breach events. The plan on how these objectives can be met should be documented in project-specific risk mitigation plans, and tracked in project reviews.

4.3 Project Generic Risk Index (PGRI)

PGRI is computed using equation (3) as shown in panel titled 'project generic risk factors assessment' in Figure 1. In this process, the project manager uses a questionnaire shown in Table 3 to assess uncertainty levels associated with each of the ten generic risk factors.

Table 3 Sample project generic risks questionnaire

Risk Index	**52.00**				
Risk Factor	*Weight*	*Rate*	*Risk Levels*	*Selection*	*Weighted Selection*
Requirements (Example Risk Levels shown)	15.00	○ 1	Clear scope and requirements	3	45.00
		○ 2	Requirements and possible changes clear		
		◉ 3	Requirements understood, may change		
		○ 4	Requirements somewhat understood		
		○ 5	Requirements not understood at all		
Solution	10.00	○ 1	Very low risk situation	2	20.00
		◉ 2	Somewhat low risk situation		
		○ 3	Medium risk situation		
		○ 4	High risk situation		
		○ 5	Very high risk situation		
Project Mgmt.	10.00	○ 1	Very low risk situation	3	30.00
		○ 2	Somewhat low risk situation		
		◉ 3	Medium risk situation		
		○ 4	High risk situation		
		○ 5	Very high risk situation		
Staffing	20.00	○ 1	Very low risk situation	5	100.00
		○ 2	Somewhat low risk situation		
		○ 3	Medium risk situation		
		○ 4	High risk situation		
		◉ 5	Very high risk situation		
Infrastructure	10.00	○ 1	Very low risk situation	2	20.00
		◉ 2	Somewhat low risk situation		
		○ 3	Medium risk situation		
		○ 4	High risk situation		
		○ 5	Very high risk situation		

Table 3 Sample project generic risks questionnaire (continued)

Risk Index **52.00**

Risk Factor	*Weight*	*Rate*	*Risk Levels*	*Selection*	*Weighted Selection*
Relationship	10.00	◉ 1	Very low risk situation	1	100.00
		○ 2	Somewhat low risk situation		
		○ 3	Medium risk situation		
		○ 4	High risk situation		
		○ 5	Very high risk situation		
Location	5.00	◉ 1	Very low risk situation	1	5.00
		○ 2	Somewhat low risk situation		
		○ 3	Medium risk situation		
		○ 4	High risk situation		
		○ 5	Very high risk situation		
Commercial	10.00	○ 1	Very low risk situation	2	20.00
		◉ 2	Somewhat low risk situation		
		○ 3	Medium risk situation		
		○ 4	High risk situation		
		○ 5	Very high risk situation		
Info. Security	5.00	◉ 1	Very low risk situation	1	5.00
		○ 2	Somewhat low risk situation		
		○ 3	Medium risk situation		
		○ 4	High risk situation		
		○ 5	Very high risk situation		
BCP/DRP	5.00	◉ 1	Very low risk situation	1	5.00
		○ 2	Somewhat low risk situation		
		○ 3	Medium risk situation		
		○ 4	High risk situation		
		○ 5	Very high risk situation		

As can be seen in the sample questionnaire of Table 3, and in the risk management process of Figure 2, project managers and risk auditors continuously monitor and report the perceived magnitude of these ten risk factors, at least once every month. An example of exact questions that may be asked has been given for factor 'Requirements'. Each question measures the level by assigning values 1 to 5, spanning levels signifying very low to very high.

Each risk factor can be assigned a weight. Weights are assigned in percentages, adding up to 100% over all. The weights are assigned by a panel of senior project managers, and are applied uniformly across all projects, irrespective of the type of project. As have been shown in Table 3 and Figure 1, exact computation can be done by adapting equation (3) as

$$\text{PGRI} = \sum_{k=1}^{10} \text{W}_k \times \text{RG}_k / L \tag{6}$$

where W_k = weight assigned to risk factor k

RG_k = value (between 1 and 5) assigned to factor k by project manager or risk auditor

L = number of magnitude levels assigned to each Risk Factor (L = 5)

In equation (3), project uncertainty is multiplied by magnitude of potential loss. It is difficult to estimate magnitude of potential loss due to project failure in the SSO context, as the potential may span from penalty, to margin loss, to loss of all future business from the customer. As can be easily understood, it is possible to take action to reduce risk factor levels. For example, if project requirements are not well understood, the mitigation action is to understand project requirements. There is not much point in estimating potential loss, as the idea is to prevent such loss through effective lowering of risk factor magnitude.

Further, multiplying the magnitude of potential loss with the uncertainty level makes it difficult to compare PGRI as a bigger project could have a larger loss potential compared to a smaller size project. Therefore we modify the equation to equation (6) to facilitate decision making.

4.4 Group Generic Risk Index (GGRI)

As discussed earlier in this paper, SSOs typically executes projects in a group, for example for a customer, or location or a domain. It is therefore necessary to devise indices to estimate aggregated risk index of projects executed in groups. These indices are termed Group Generic Risk Index (GGRI). GGRI is the *N*th percentile (N is typically 80) of all PGRIs of projects in the group. Percentile method is superior compared to arithmetic average as averages often present misleading risk factor levels.

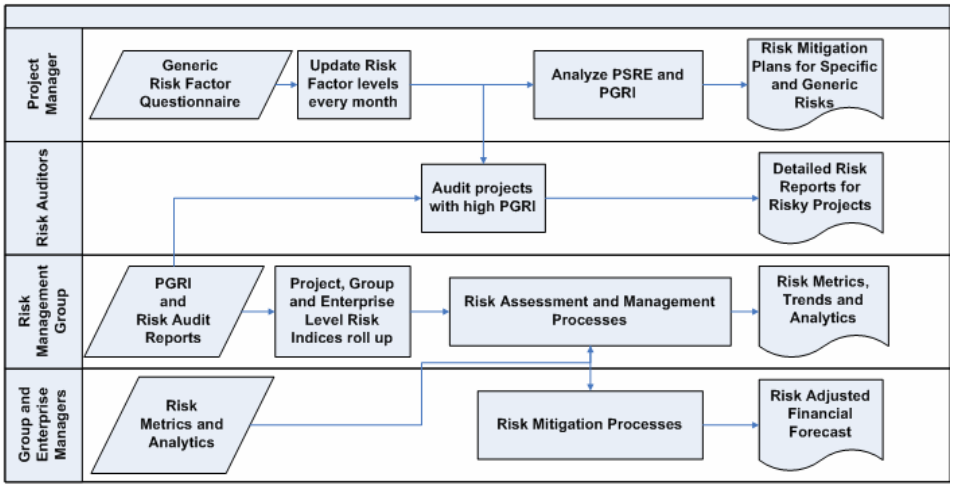
4.5 Enterprise Generic Risk Index (EGRI)

Rolling up GGRIs and taking the *M*th percentile point (*M* is typically 80) can similarly compute EGRI. *N* and *M* can be kept at the same value. Figure 1 describes the process fully.

4.6 Workflow system

A workflow to use the computational framework is presented in Figure 2. Project managers fill in project-specific risks, probabilities and consequences in a risk management system. They also report generic risk factor scores using the risk management system, once every month. The system computes PGRI, GGRI and EGRI. These indices are used by trained risk auditors to identify projects with high risk (probability of showing high margin loss) and subsequently subjecting these projects (or sometimes, groups) to detailed and frequent audits. Through analysis of the resultant risk metrics and reports, detailed mitigation plans are prepared and executed at project, group and enterprise levels.

Figure 2 Risk assessment and mitigation workflow (see online version for colours)



5 SSO operational risk indices and risk management system: a case example

A 'Mid-sized Software Services Company' (MISCO) is one of the leading global providers of IT services and business solutions. Several thousand professionals service clients across diverse industries, from sales offices across USA, Europe and Asia-Pacific, and Global Delivery Centres located in many countries. MISCO has serviced numerous Fortune 1000 companies, for over two decades.

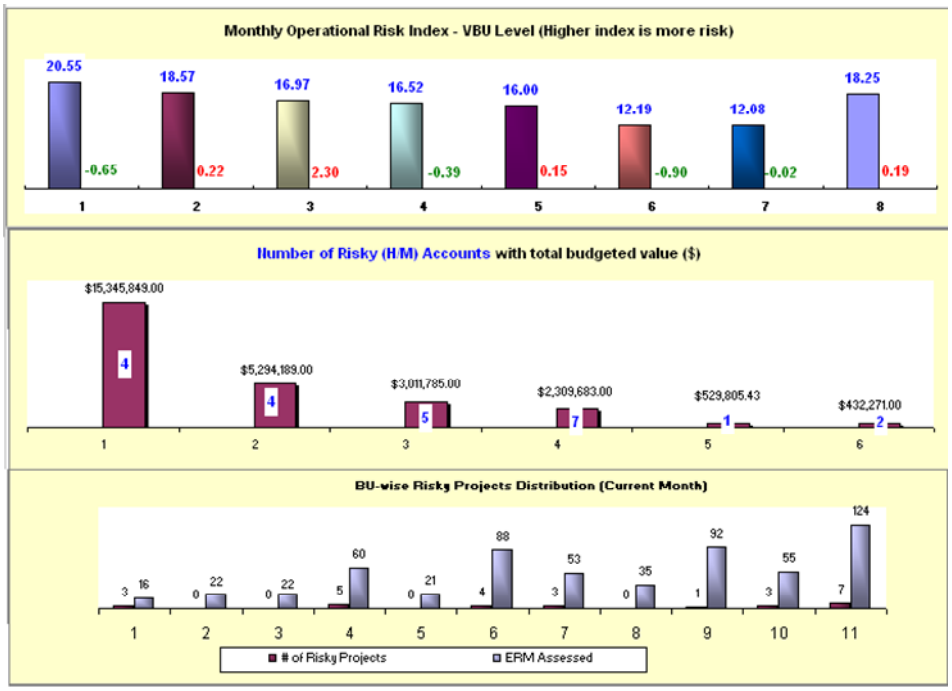
Possibility and magnitude of margin loss therefore is the 'risk' that MISCO is trying to minimise. It has been established at MISCO that there exists a significant correlation between the magnitude of risk factors identified in Table 2 and Margin Loss defined in equation (4).

MISCO is an ISO 9000 (International Standards Organization, www.iso.org) certified company. It has also been assessed at level 5 of SEI/CMMi (Integrated Capability Maturity Model of the Software Engineering Institute, www.sei.cmu.edu). All projects follow formal risk management and mitigation methods. Most of the project managers have received formal training in project management, and several have formal project management certifications from Project Management Institute (www.pmi.org) and others. All managers have knowledge about formal software engineering processes and models.

The risk management computational system and workflow using the operational risk indices presented earlier has been deployed and validated at MISCO for more than two years since 2007. The model is now fully validated having been used on more than a thousand projects of all types described in Section 5.

Sample risk dashboards are shown in Figure 3. BU in the figure means 'Business Units'. Risky (H/M) refer to High and Medium risk projects, a classification introduced to distinguish between the risk levels of risky projects.

Figure 3 Sample MISCO risk dashboards (see online version for colours)



5.1 *Significant findings*

Some of the significant findings are presented briefly as follows:

- It was found that high PGRI (and consequently GGRI) provides very effective risk forewarning to management, allowing corrective and preventive mitigation actions well in time. The indices failed to provide forewarning only for .02% (2 projects per 1000 projects) of the active projects, on yearly basis.
- MISCO EGRI has come down by 7 points in two years. This reflects effective assessment and mitigation actions on generic risk factors across the entire enterprise.
- Monthly risk mitigation rate, defined as the percentage of risky projects that have been brought out of high risky zone, averaged 20%. This means that a fifth of the projects that were assessed as having a high probability of margin loss were prevented from losing margin every month.

- Analysis of these various risk indices allowed MISCO to identify organisation-wide improvement areas. Effects of these improvements were clearly evident on GGRI and EGRI.
- Over 99% of the managers use the automated risk management system every month, providing reliable and current PGRI, and allowing computation of GGRI and EGRI.
- These indices were able to provide ample forewarning to management about the projects that were likely to fail in meeting project objectives. Success rate achieved in forewarning was 99.98% per annum, or 2 projects per 1000 per year. The indices allowed management to initiate corrective and preventive actions in time at project, and organisation levels, leading to reduction of risk indices across various business units and projects.

6 Concluding remarks

This paper introduces the concept of software project generic risk factors, and proposes that SSO-related standards and quality frameworks should include the concept of generic risk factors. It also represents a case example and derives significant learning out of application of a risk management framework. Case example represents a major global player in the software services outsourcing industry, where the business dimensions in terms of project management are circumscribed by multiple variety and widespread diversity. Therefore, the example itself demonstrates the current realities of the contemporary SSO industry. Therefore, the significant learnings of the case are generalisable and have transferability to other companies. Apart from these, this paper presents a set of ten software project risk factors that apply to projects of all types commonly found in SSO industry. A computational system framework that can estimate both project-specific and generic risk factors have been developed and validated. A workflow system that can be deployed by SSO industry to exploit this computational framework to manage software project risks through multi-criteria decision making, and divert multiple scarce resources to projects most in need have been designed. It also allows SSO industry management to undertake project-specific, group level and enterprise level corrective and preventive risk mitigation actions on time. By using this framework, MISCO has experienced prevention of substantial losses. Existing IT and SSO-related standards do not mandate use of generic project risk factors, and focus entirely on project-specific risk factors. The computational and workflow system framework developed and validated in this paper can be incorporated in relevant standards. This would deliver tremendous value to the global SSO industry.

SSO is a major industry and very rapidly growing and generating huge revenues across the world. It also provides employment to millions of young talents. Continued well-being of this industry would require these enterprises to reduce costs through prevention of losses. Effective risk identification and prudent use of risk management techniques will help SSO industry in achieving the objectives of cost reduction and loss prevention. Although the risk management systems based on the indices presented in this paper have been found to be effective at MISCO, it is felt that the PGRI computation can be made more effective if Fuzzy Set based methods are used instead of crisp numbers (Cong et al., 2008).

Acknowledgements

We gratefully acknowledge the insightful comments and feedbacks of the anonymous reviewers that allowed us to make this paper more value adding. The authors would also like to sincerely thank MISCO for permitting the use of related information.

References

Barki, H., Rivard, S. and Talbot, J. (1993) 'Toward an assessment of software development risk', *Journal of Management Information Systems*, Vol. 10, No. 2, pp.203–225.

Beasley, M., Bradford, M. and Pagach, D. (2004, July) 'Outsourcing? At your own risk', *Strategic Finance*, pp.23–29.

Boehm, B. (1989) *Software Risk Management*, IEEE Computer Society Press.

Boehm, B.W. and DeMarco, T. (1997) 'Software risk management', *IEEE Software*, May/June, pp.17–19.

Brandas, C. (2010) 'Risk and audit objectives for IT outsourcing', *Informatica Economica*, Vol. 14, No. 1, pp.113–118.

Brown, D. and Wilson, S. (2007) *Black Book of Outsourcing*. Available online at: www.theblackbookofoutsourcing.com

COSO (2004) *COSO Enterprise Risk Management – Integrated Framework*. Available online at: www.COSO.org

Chandra, P. (2003) *Finance Sense – Finance for Non-Finance Executives*, 3rd ed., Tata McGraw-Hill Publishing Company Limited, New Delhi.

Cong, G., Zhang, J., Chen, T. and Lai, K. (2008) 'A variable precision fuzzy rough group decision-making for IT offshore outsourcing risk evaluation', *Journal of Global Information Management*, Vol. 16, No. 2, pp.18–34.

Copas, J. (1999) 'Statistical modeling for risk assessment', *Risk Management: An International Journal*, Vol. 1, No. 1, pp.35–49.

Dasgupta, J. and Mohanty, R.P. (2009) 'Towards evaluating the risks of software services outsourcing industry', *Vilakshan: XIMB Journal of Management*, Vol. 6, No. 2, pp.29–48.

Davies, P. (2004) *What's this India Business? Offshoring, Outsourcing and the Global Services Revolution*, Nicholas Brealey International, UK.

Escobar, M. and Seco, L. (2008) 'The mathematics of risk transfer', *International Journal of Services Sciences*, Vol. 1, No. 1, pp.21–35.

Ethiraj, S., Kale, P., Krishnan, M.S. and Singh, J.V. (2005) 'Where do capabilities come from and how do they matter? A study in the software services industry', *Strategic Management Journal*, No. 26, pp.25–45.

Fight, A. (2004) *Credit Risk Management*, Butterworth-Heinemann, USA.

Gefen, D., Wyss, S. and Lichtenstein, Y. (2008) 'Business familiarity as risk mitigation in software development outsourcing contracts', *MIS Quarterly*, Vol. 32, No. 3, pp.531–551.

Jiang, J., Klein, G. and Ellis, T.S. (2002) 'A measure of software development risk', *Project Management Journal, Project Management Institute*, Vol. 33, No. 3, pp.30–41.

Kakumanu, P. and Portanova, A. (2006) 'Outsourcing: its benefits, drawbacks and other related issues', *The Journal of American Academy of Business, Cambridge*, Vol. 9, No. 2, pp.1–7.

Kasiri, N.A. and Sharda, R. (2008) 'Some now, some later? Selecting a 'lot size' of e-mails to process at one time', *International Journal of Services Sciences*, Vol. 1, No. 1, pp.69–82.

Koong, K.S., Liu, L.C., Bai, S. and Wei, J. (2008) 'Occurrences of Internet fraud in the USA', *International Journal of Services and Standards*, Vol. 4, No. 1, pp.33–53.

Kutsch, E. (2008) 'Thesis report note on the effect of intervening conditions on the management of project risk', *International Journal of Managing Projects in Business*, Vol. 1, No. 4, pp.602–610.

Lam, J. (2003) *Enterprise Risk Management, From Incentives to Controls*, John Wiley & Sons, Inc., USA.

Leung, H.K.N. (1995) 'A practical risk index', *Transactions on Information and Communications Technologies*, Vol. 11, pp.215–226.

Miller, R.E., Hardgrave, B.C. and Jones, T.W. (2008) 'Levels of analysis issues relevant in the assessment of information systems service quality', *International Journal of Services and Standards*, Vol. 4, No. 1, pp.1–15.

Mulcahy, R. (2003) *Risk Management – Tricks of the Trade® for Project Managers, A Course in a Book™*, RMC Publications, Inc., USA.

Nargundkar, R. (2008) *Marketing Research, Text and Cases*, 3rd ed., Tata McGraw-Hill, New Delhi.

NASSCOM (2008) *Indian IT-BPO Analysis*. Available online at: www.nasscom.org

Taylor, H. (2007) 'Outsourced IT project from the vendor perspective: different goals, different risks', *Journal of Global Information Management*, Vol. 15, No. 2, pp.1–27.