Communications of the Association for Information Systems

Volume 13 Article 20

February 2004

Technical Risk Management on Enterprise Integration Projects

Wing Lam
UNiversitas 21 Global, Wing.lam@U21Global.com

Recommended Citation

Lam, Wing (2004) "Technical Risk Management on Enterprise Integration Projects," *Communications of the Association for Information Systems*: Vol. 13 , Article 20.
DOI: 10.17705/1CAIS.01320
Available at: https://aisel.aisnet.org/cais/vol13/iss1/20

Communications of the Association for Information Systems

TECHNICAL RISK MANAGEMENT ON ENTERPRISE INTEGRATION PROJECTS

Wing Lam
Universitas 21 Global
Wing.lam@U21Global.com

ABSTRACT

Enterprise Integration (EI) is essential to organisations wishing to fulfill broader business objectives related to e-business, customer relationship management (CRM), supply chain management (SCM) and business-to-business (B2B) commerce. This paper describes and presents the results of a study into practices for managing technical risk on EI projects. In the study, 21 managers participated in a facilitated workshop or interview sessions to identify areas of risk (RAs) associated with EI projects and risk management practices (RMP) for addressing those RAs. Risks were identified in four separate phases in the lifecycle of an EI project, namely the strategy, planning, implementation and rollout phases. Many of the risks identified were not specific to EI projects, but were applicable to large IT projects in general. The paper is primarily concerned with technical risk although some aspects of business and organizational risk are discussed briefly.

Keywords: risk management, technical risk, enterprise integration, EAI, systems integration.

I. INTRODUCTION AND MOTIVATIONS

IMPORTANCE OF ENTERPRISE INTEGRATION (EI)

The need to integrate IT systems within the enterprise, and sometimes between different enterprises, is a major challenge in the IT industry today. Enterprise Integration (EI) is normally essential to organisations wishing to fulfill broader business objectives related to e-business, customer relationship management (CRM), supply chain management (SCM) and business-to-business (B2B) commerce. Most e-business, CRM, SCM and B2B projects are characterised by significant amounts of EI work that involve integrating packaged applications (such as SAP R/3, Siebel and Peoplesoft), legacy applications (based on mainframe technology such as CICS and MVS), custom applications, and database management systems (such as Oracle, DB2 and MS SQL Server).

PAPER OBJECTIVES

This paper describes and presents the results of a study into practices for managing technical risk (but not other risks such as business or organizational risk) on EI projects. In the study, a group of project managers and solution architects from a large, well-respected international IT consultancy firm, referred to here as 'Firm X', participated in a facilitated workshop to identify areas of risk (or RAs for short) associated with EI projects and risk management practices (RMPs) for avoiding, mitigating or minimizing risks in those RAs. Following the workshop, further interviews were conducted with several of the project managers within the group, and business managers representing client organizations of Firm X.

The outline of the paper is:

Section II, presents an overview of EI and its challenges.

Section III describes the motivations for the study and provides background on Firm X.

Section IV discusses the research methodology.

Section V presents the results of the study in terms of the RAs and RMPs identified.

Section VI summarizes the findings from our study and presents a framework for risk management based on the findings.

Section VII concludes by highlighting the contributions of the paper, and discusses potential areas for future research.

II. ENTERPRISE INTEGRATION OVERVIEW

TYPES OF EI PROJECTS

The term 'EI project' is used here to refer to any IT project that involves a significant amount (more than 35% of the total effort) of EI-related work. EI-related work includes business process modeling, application integration, middleware design and development, and integration testing. EI projects generally fall into one of four main categories:

- **Enterprise application integration (EAI).** The integration of IT systems within an enterprise, typically to improve business efficiency and to meet needs for real-time information processing.

- **Web integration.** The integration of legacy systems with Web-based applications, driven by a need to provide customers with a web channel for accessing products, services, or information.

- **B2C integration.** The integration of back-end transactional IT systems, which may be legacy in nature, with Web-based front-end applications such as storefronts and personalization engines to provide B2C solutions.

- **B2B integration.** The integration of IT systems between different organisations to support B2B activities such as integrated supply chain management.

EAI projects might be considered a modern-day evolution of what were traditionally known as 'systems integration' (SI) projects. However, whereas SI projects tended to focus on point-to-point integration between IT systems, EAI addresses the problem on a scale where there are tens, even hundreds of IT systems to be integrated. Web integration, B2C, and B2B projects are now common because of the adoption of e-business and the increasing use of the Internet by organisations to deliver, provide, or support business services.

CHALLENGES

The challenges associated with large-scale IT projects that can increase their level of risk are discussed in Keil et al. [1998] and Whittaker [1999]. Ten of the specific challenges inherent to EI projects are listed in Table 1.

LEVELS OF INTEGRATION

As well as the type of EI project, the level of integration is another dimension that distinguishes one project from another (Figure 1).

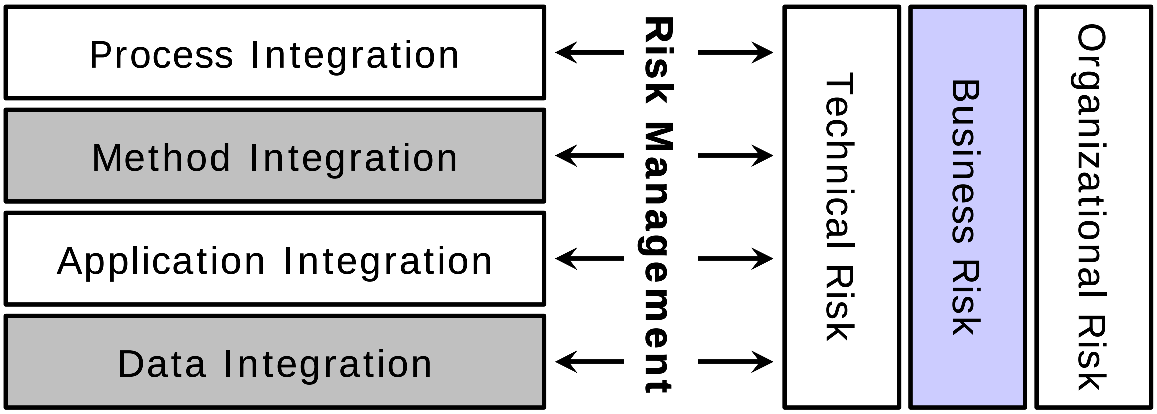


Figure 1. Levels of Integration and Types of Risk

The diagram on the left-hand side illustrates the four different levels at which integration can be achieved, based on Linthicum [2001], with the higher levels building on top of the lower levels. The right-hand side of the diagram indicates the three different types of risk that need to be managed, technical, business or organizational risk. This paper is largely concerned with the management of technical risk, although some discussion of business and organizational risks is included in the paper.

Data integration is largely concerned with the synchronisation of data held in different databases. Synchronization can be achieved either in real-time, or in batch mode where some temporary delay in data freshness is permissible to the enterprise.

Application integration is concerned with enabling applications to directly access functionality of other applications in a real-time fashion. Popular packaged applications such as SAP and PeopleSoft, for example, provide well-defined application programming interfaces (APIs) that expose the functionality within the application.

Method integration is concerned with providing applications with a common set of reusable business logic from which finer grain application calls are made. For example, reusable business logic for creating a new customer may trigger separate customer creation processes in several different applications. At this level, there is a clean separation of business logic from the technical means by which systems are integrated.

Process integration is concerned with the abstraction and definition of business process or workflow models from which relevant methods are called. Process integration is particularly relevant in collaborative contexts, such as B2B, where there are significant business information flows between trading partners. More discussion on the levels of integration can be found in Linthicum [2001].

Table 1. Specific Challenges Inherent in EI Projects

Type of Challenge	**Nature of Challenge**
Standalone Designs	The requirement to integrate IT systems that were originally designed to be standalone. In such cases, the original application often needs to be substantially re-engineered or extended so that an external interface can be provided.
Heterogeneous technologies	The IT systems to be integrated reside on different platforms, employ different technologies and programming languages, and are distributed in nature. Such technological diversification tends to heighten technical complexity.
Heterogeneous organizations	The organization's business policies and processes are incompatible, or in conflict with, the business policies and processes of other organizations. Such issues are particular relevant in merger and acquisition scenarios.
Legacy engineering	Legacy IT systems that use old, outdated and possibly unsupported technology need to be integrated. Understanding the limitations of the legacy technology and how well it can be made to interact with more modern technologies is often a major area of uncertainty, particularly when the modern technologies are themselves evolving. In addition, finding individuals with appropriate legacy engineering skills can be problematic.
Poor documentation	When IT systems are poorly documented, understanding the internal design of systems is difficult, and any 'invasive' integration work that affects the internal working of the application potentially damaging.
Interface limitations	Where applications do have published interfaces or APIs, they are restricted in functionality, performance, reliability, or mandate the use of a particular programming language such as C++.
Scale of integration	Large organisations run many hundreds, possibly thousands of distinct IT applications. Understanding the set of feasible integration options for each of these IT applications, and how they can be incorporated into overall integration architecture requires considerable effort.
Semantic mismatch	Syntactic and semantic differences exist in the interpretation of data by individual IT systems. Data must not only be shifted from one application to another, but also transformed in a way that can be readily consumed by others.
Need for real-time response	The need to provide real-time information and services means that simple integration solutions based on batch processing and export-transfer-load approaches are not feasible. Instead, solutions based on more sophisticated, and inherently more complex, integration technologies must be architected.
Application-specific security models	IT applications use their own individual security model (authentication, authorization, auditing etc.), which is not typically exposed to other applications. The lack of an acceptable architecture-wide security model can become a serious project impediment.

Early EI solutions tended to focus on point-to-point integration between specific IT applications either at the data or application level. However, more flexible EI solutions based on message-oriented-middleware (MOM) and integration brokers have emerged, and aggressively marketed by vendors such as IBM (Websphere Business Integration Suite), TIBCO (Integration Broker), WebMethods (WebMethods Integration Platform) and Vitria (BusinessWare). More recently, these solutions included business process modelling and workflow functionality to enable process integration. Web services have also surfaced as an important technology for achieving interoperability between IT systems in a loosely coupled and platform-independent manner. More detailed descriptions of EI business drivers, architectures, and technology, are presented in McKeen and Smith [2002], Linthicum [2001] and Cummins 2002.

III. STUDY MOTIVATIONS AND BACKGROUND

FIRM X SOLUTION CENTRES

The technology solutions centres (TSC) within Firm X are involved in many EI projects that involve the design and delivery of large-scale IT solutions for a range of client organisations across many vertical industries. Information about Firm X and the TSC that collaborated in our study is shown in Sidebar 1.

SIDEBAR 1. DETAILS ON FIRM X

- Firm X is a global management consulting, technology services and outsourcing company.
- Services lines include strategy, customer relationship management, supply chain management, solutions engineering and solutions operation.
- Over 50,000 employees worldwide.
- Vertical industries include communications and high technology, financial services, government and utilities.
- Over 20 TSCs around the world.
- The staff of the TSC involved in the study is over 450people, one of the largest of its kind.
- The working experience of over 70% of the staff at the TSC is 5 or more years.

Over the last 5 years, Firm X undertook a significant number of EI projects; many of these projects were in the areas described in Figure 2.

Some EI projects involve TSCs undertaking the entire EI work for the client, normally as part of a broader project engagement, or as a distinct piece of outsourced work. In other cases, TSCs work with vendors as part of a joint EI team. It is not uncommon to see consultancies like Firm X working with both middleware vendors and application vendors on the same EI project for a client.

Some of the roles that individuals within the TSC may undertake in a client engagement are shown in Table 2 together with an indication of the areas of risk typically faced by individuals in those roles.

In a scenario where the client outsources all the integration work, TSC staff can expect to fulfill all the above roles. In a scenario where the client organization requested consultancy, TSC staff can be expected to work alongside staff in the client organization.

Financial Straight Through Processing (STP)	The integration of front-office, middle-office and back-office systems so that financial transactions can be processed within minutes rather than days. STP allows trades to be input only once, rather than in several IT systems, so greatly reducing the margin for human error and enabling greater processing throughput.
E-Government Citizen Services	The provision of citizen services, traditionally conducted through manual, face-to-face channels, to an online, Web-base channel. E-Government projects typically involve integration with 10-20 year old legacy applications and major business process re-engineering activities.
Customer Relationship Management and Call-Centre Solutions	The creation of customer service solutions that typically centre around the integration of off-the-shelf customer relationship management (CRM) packages and call-centre solutions. Customer details and records can be accessed from a single interface, even though they be may be physically stored in several different systems.
Integrated Healthcare Solutions	The need for centralized patient records and sharing of patient information between individual healthcare systems is fuelling an increasing demand for integration projects within the healthcare industry. More advanced projects involve real-time integration between clinical systems as well as patient record systems.
Web-based access to Internal Business Services	Many organizations have existing systems that provide services that serve internal business needs, but which are either difficult to access, or accessible only through archaic client interfaces. Integration projects here typically centre around developing portals and intranet solutions that provide browser-based access to these internal business services.

Figure 2. Types of Enterprise Integration Project Undertaken by Firm X

Table 2. Roles and Risks in Firm X Projects

Role	***Role Description***	***Areas of Risk***
Program managers	Responsible for the overall health of a project engagement with a client and the overall management of individual projects that fall within the program.	Client confidence and support, contribution to business value.
Project managers	Manage teams of people on an EI project. This not only includes technical managers, but individuals who manage business areas such as B2B strategy.	Project completion and schedule, project budget, project resourcing, scope creep.
Solution architects	Take a leading role in helping the client organization architect a holistic solution and determining the integration architecture..	Poor solution performance, shortfall in meeting functional requirements, poor reliability, excessive operations management and maintenance.
Data architects	Responsible for the development of the enterprise data architecture, identifying data sources and repositories, and the distribution of data within an organization.	Data redundancy and inconsistency, poor data quality.

Business process analysts	Engaged in activities relating to the modeling of existing business processes used within an organization, business process re-engineering and the development of new business processes.	Inefficient business processes, poorly performing and non-scaleable business processes.
Change management consultants	Responsible for the transitioning to the new EI solution including designing new organizational structures, and revising roles and responsibilities.	Lack of clear organizational roles and responsibilities, weak transition plans.

STUDY MOTIVATIONS

The author, with support from management sponsors within Firm X, undertook a study to investigate practices for managing risks on EI projects as part of the sharing best practices ethos that is strongly encouraged within the firm. The motivations for the study were:

EI work was becoming an integral part of almost all projects conducted within the TSCs of Firm X. Increasingly, integration work is no longer considered by clients as ‘behind-the-scenes’ technical ‘plumbing’ work, but as a strategic IT imperative upon which key business initiatives depend.

EI work is becoming increasingly complex, both in terms of the integration problem (the number and nature of IT systems that need to be integrated) and diversity of integration solutions that can be used (e.g., middleware, integration brokers, Web services, XML). This complexity tends to increase project risk.

- EI work can prove very costly if it spirals out of control. EI solutions can be built that don’t meet their expectations, or fail to reach a state of completion altogether. In addition, EI work often requires specialised integration and middleware skills that command premium fees.

- The ability to deliver EI projects on time and within budget is dependent upon the project management and solution architecture teams within the TSCs of Firm X being effective in negotiating and managing risks on EI projects. To help achieve this goal, a set of practical risk management strategies needs to be formalised.

EXISTING LITERATURE

A literature review was conducted prior to the study itself. The risk management literature is extensive. Much of the literature discusses methodologies and systematic processes for managing risk, particularly in a software engineering context, including spiral and iterative models of software development [Boehm 1989], risk specification and analysis toolkits [Gilb 2002], risk management methodologies [Fairley 1994; Myerson 1996; Sage 1995], and risk evaluation methods [Sisti and Joseph 1994]. In addition, automated tool support for risk management, including risk analysis using groupware [Weatherall and Hailstones 2002)], risk assessment using systems dynamics modelling [Mawby and Stupples 2002], risk modelling [Roy and Woodings 2000; Cornford et al. 2001], and risk estimation and documentation [Keshlaf and Hashim 2000] are discussed in the literature.

Other work has attempted to identify and categorise risk factors, or what I call risk areas (RAs), in software engineering projects. Notable work here includes Boehm’s [1989] top 10 risk areas in software engineering, the Software Engineering Institute’s software development risk taxonomy [Carr et al. 1993] and Murthi’s [2002] risk categories. Other work attempts to identify risk factors on specific types of project, e.g. Internet and Intranet software projects [Reifer 2002] and ERP projects [Sumner 2000]. The practices used by IS managers to manage risk on IS projects, what I call risk management practices (RMP), was investigated by Smith et al. [2001)]. However, little attention is given to risk factors or risk management practices specific to EI projects.

As indicated in Section I, this study focuses primarily on technical risk on EI projects. More detailed discussions on business and organizational risk can be found elsewhere [Simons 1998; Elkington and Smallman 2002]. More specifically, Zsidisin [2003] examines the risks in supply chain management; Wright and Wright [2002] the risks in implementing ERP solutions; Buchanan and Connor [2001] the organizational risks associated with large IT projects. In addition, Schneier and Miccolis [1998] propose ‘Enterprise Risk Management’ as a distinct practice for managing all of an organisation’s key risks at an enterprise level.

STUDY OBJECTIVES

Following initial discussions between the author and Firm X management sponsors, the main objectives of the study were formalized as:

- **Risk areas (RAs).** To understand and identify the areas and factors that contributes to increased risk on EI projects. The predominant focus was on technical risk, although some business and organizational risk is also covered..

- **Risk management practices (RMPs).** To identify risk management practices (RMPs) that can be applied by project managers and IT solution architects to avert, mitigate or minimise risk on EI projects.

The management sponsors emphasised that the study should be grounded in real-world experiences from TSC consultants actively working ‘in the field’ of EI projects, rather than on abstract or theoretical models. As such, it was agreed that the main format for the study should be based around a facilitated workshop with selected consultants working within TSCs.

IV. STUDY METHODOLOGY

METHODOLOGY STEPS

The methodology used for our study involved six steps:

1. *Create a lifecycle model for enterprise integration projects (LEIP).* The author anticipated that different kinds of risks would arise at different stages in the lifecycle of an EI project. A lifecycle model for EI projects (LEIP) was therefore created first, derived largely from the author’s previous work (Lam and Shankararaman 2004). LEIP is described in the next subsection.

2. *Target group identification.* A target group of 32 consultants within TSCs of Firm X were identified individuals who could participate in the study. The target group was selected on the basis of their experience (5 years or more IT working experience) and current engagement on an EI project. It was believed that junior consultants, with less than 5 years IT experience, would be unlikely to assume project management or solutions architect roles where they would have sufficiently broad exposure to EI issues. No attempt was made to include or exclude certain industry sectors or type of EI projects because the study was meant to identify risks and strategies that would apply across all EI projects. Of the target group, 19 individuals out of the 32 agreed to participate in our study following an email request outlining the objectives, the format of the study, and their expected commitment.

3. *Workshop preparation.* I invited the 19 who agreed to participate to a facilitated workshop. As part of the workshop preparation, I emailed the group the LEIP I created earlier to provide them with a framework to centre their thinking around. In addition, I sent them a set of ‘facilitation questions’ that was representative of the type of questions I would be using in the workshop. As the workshop was discussion-oriented, I expected the generation of ideas to be spontaneous, but using facilitation questions to anchor the discussion. The facilitation questions are describedin the subsection after next.

4. *Workshop execution.* 16 out of the 19 who had agreed to participate in the study actually turned up to the workshop. As some of these individuals were currently working on the same project, a total of 12 separate individual projects were represented. The workshop was conducted over one full day and led by the author.. The first phase (1 hour) was devoted to introductions, recap of study objectives, format and outcomes and overview of the LEIP model. In the second phase (45 minutes), I asked one of the participants to give a presentation describing EI experiences on his current project. This presentation served as a lead into the actual discussion itself. The third phase (2-hour) involved discussion over the first half of the LEIP model, during which risk areas (RAs) and risk management practices (RMPs) were identified. Similarly, the fourth phase (2-hour) involved discussion over the 2nd half of the LEIP model. After the third and fourth phases, workshop facilitators (two research assistants) structured the discussion outputs into a more organised and coherent form, which was then presented back to participants in the fifth phase (1.5 hour) for their review and comment. Long (30 minute) breaks punctuated phases to promote personal discussion, sharing between workshop participants and to allow sufficient periods for rest.

5. *Results compilation and review.* After the workshop, the author spent several days conducting a more detailed analysis of the workshop transcripts and outputs. This analysis allowed the author to formalise and elaborate on ideas that existed in ‘skeleton’ form, and establish relationships between ideas. The results from this activity was drafted in a white paper, which was subsequently emailed to the participants that attended the workshop for their comments or any further thoughts about the workshop. Their feedback was incorporated into a final version of the white paper that was released on Firm X’s internal KM system and forms the basis upon which the present article is based.

6. *Follow-up interviews.* Acting on feedback from one of the paper’s reviewers, a follow-up activity was conducted to elaborate further on the business and organizational risks associated with EI projects. Four of the project managers in the original group were interviewed as were 5 business managers from three client organizations of Firm X.

In terms of study duration, step 1 to 5 took approximately 12 weeks, and step 6 a further 3 weeks. Of the total 21 project managers, business managers and solution architects who participated in the study, 19 provided work-related data about themselves, as summarized in Table 3.

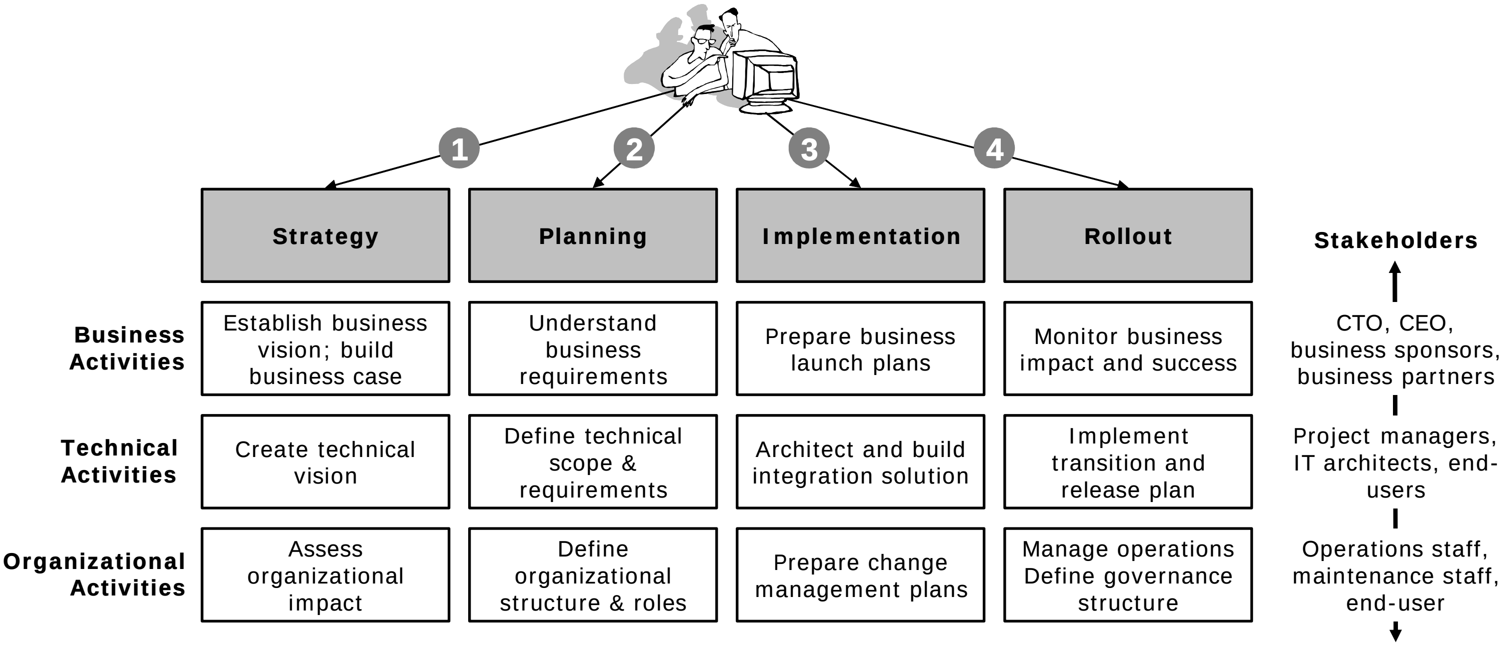
Table 3. Participant Demographics

- Average number of years work experience: 18-19 years.
- Average number of years in current organization: 8-10 years.
- Average number of years working on projects involving significant EI work: 6-8 years.
- % of participants in area of Management: Technical: 63%; Business:32%; Other: 5%.
- % of participants with experience of EAI: 89%.
- % of participants with experience of Web Integration: 74%.
- % of participants with experience of B2C: 74%.
- % of participants with experience of B2B: 32%.

In summary, all the participants in our study were seasoned IT professionals with significant experience of EI projects.

LEIP

The lifecycle model for EI projects, named LEIP, was created as part of the step 1 in our research methodology to provide workshop participants with a framework for structuring their thinking. The LEIP is shown diagrammatically in Figure 3, and is largely self-explanatory.



	Strategy	Planning	Implementation	Rollout	Stakeholders
Business Activities	Establish business vision; build business case	Understand business requirements	Prepare business launch plans	Monitor business impact and success	CTO, CEO, business sponsors, business partners
Technical Activities	Create technical vision	Define technical scope & requirements	Architect and build integration solution	Implement transition and release plan	Project managers, IT architects, end-users
Organizational Activities	Assess organizational impact	Define organizational structure & roles	Prepare change management plans	Manage operations Define governance structure	Operations staff, maintenance staff, end-user

Figure 3. Lifecycle Model for Enterprise Integration Projects (LEIP)

LEIP takes influences from previous work on EI methodologies [Lam and Shankararaman 2004; Ruh et al. 2001], as well as input from two seasoned EI project managers within TSC. The LEIP shown here is an updated version from the one actually used on the study, but the essence remains largely the same. The LEIP consists of four main phases:

- **Strategy**—The CTO, or someone in an equivalent position, with support from business stakeholders, establishes the business vision that is the pretext for EI, e.g. e-business or CRM. The CTO also prepares the business case that justifies the EI project.

- **Planning**—Programme managers translate the business strategy into a defined programme of work, establish the scope of integration projects (or sub-projects), identify relevant partners, and mobilize resources accordingly.

- **Implementation**—Project managers, architects and developers carry out the integration project. This work normally involves business process analysis, the gathering of requirements from stakeholders, architecting and implementing an integration solution, and testing.

- **Rollout**—The integration solution is rolled out into the live environment as part of the release management effort. Any associated transition or change management plans are executed.

In LEIP, I view all EI projects in terms of these four basic phases, though in practice individual projects may emphasise different phases to a greater or lesser degree, e.g. a project may be more focused on the planning, implementation and rollout of an EI solution rather than on the strategy phase.

FACILITATION QUESTIONS

I indicated earlier that a set of facilitation questions was sent out to workshop participants with the LEIP as part of their workshop preparation (step 3). The facilitation questions were as follows:

- What aspect of your current project is concerned with EI work?

- In your experience, what are the problems and issues related to the creation of an appropriate strategy for enterprise integration (EI), and how should such problems be addressed?
- In your experience, what are the problems and issues related to project planning and management for EI work and activities, and how should such problems and issues be effectively managed or resolved?
- In your experience, what are the problems and issues related to architecting, designing and implementing an EI solution, and how should such problems and issues be effectively managed or resolved?
- In your experience, what are the problems and issues related to rolling out an EI solution, and how should such problems and issues be effectively managed and resolved?
- What are the other key challenges associated with the delivery of EI solutions?

By focusing attention on problems and issues that participants faced, or were currently facing on their project, it was believed that the risks associated with EI projects would naturally emerge.

PARTICIPANT CASE-HISTORIES

During the workshop itself, many participants made reference to previous projects that they worked on when responding to the facilitation questions. These previous projects are essentially the case-histories from which our study findings are derived. A flavour of these case-histories is given in Table 3.

Table 3. Three Case Histories

Participant:

An Associate Partner who has worked on large government projects in the UK for the last 15 years.

Projects:

Employment benefits system, employment taxation system, local business registry, various local e-government portals.

Major Risks Noted:

- Government departments generally work in silos, and are often unwilling to share information with other government departments unless they receive a specific mandate.
- Government departments are often driven by internal administrative goals rather than customer-focused ones. Consequently, the motivations for EI projects are often rooted in only making administrative improvements.
- The inherent culture of the civil service is change averse. EI projects that require significant and sweeping changes in process enactment are prone to failure simply because of worker resistance to change even when management gives full support.
- Care should be taken to check whether or not an EI project creates any ‘hidden’ impact on national or local government policy and regulation. A project immediately becomes high risk if it interferes or somehow changes the nature by which decisions are made.

Participant:

A senior project manager specializing in call-centre, customer support, and customer relationship management (CRM) solutions

Projects:

Call-centre and customer support solutions for a large insurance firm, mortgage broker and a major high-street bank.

Major Risks Noted:

- Call-centre and CRM solutions are typically based on packaged IT solutions such as Seibel. Most problems occur in the technical integration between the packaged IT solutions and existing IT applications.
- Integration with legacy DB applications is a major area of risk because of incompatibilities in file formats and the inherent limitations of older platforms. In some cases, the addition of middleware processing can resolve such issues, but typically requires custom development which adds to the cost of a project.
- Understanding data architecture and the ownership of data across the enterprise is important as a tool in managing the political risk that often exists between different organizational units.

Participant:

A senior project manager involved in EI projects for large organizations in the manufacturing sector.

Projects:

Supply chain management (SCM) and ERP projects, EDI project, B2B project for automotive parts trading.

Major Risks Noted:

- The vision of an integrated SCM solution is seductive. However,it is often difficult to translate this vision into a defined architecture of integrated systems in the end-to-end supply chain of an organisation. Not having a clear Integration architecture puts a project at major risk.
- For SCM or B2B to succeed, a shared and precise definition of the trading processes that different suppliers and buyers will conform to is needed. Without these definitions, integration projects tend to drag on and on.
- Transitioning from a non-integrated supply chain to an integrated or partially integrated one requires meticulous planning because a whole host of systems such as inventory, warehousing, logistics and order management systems need to be switched over at the same time. A poorly thought out transition plan puts a project, and organization, at high risk.

V. STUDY RESULTS

The next four subsections describe the the RAs and RMPs that relate to the LEIP that emerged from the workshop and follow-up interviews. Individual risk areas are identified by a ‘RA’ coding (RA-S*n* indicates a RA in the Strategy phase where *n* is a number). Although I am largely concerned with technical risk in this paper, I indicate if the risk is of a business, technical or organizational nature, or indeed a combination of several types of risk. For each RA, a set of risk management practices (RMPs) is suggested. These practices can either be used in pre-emptive mode to avert problems occurring in the first place, or in reactive mode to control or rescue problematic situations. Many risks are inter-related, which is why certain RMPs can be used to address multiple RAs.

RISK MANAGEMENT IN THE STRATEGY PHASE

RA-S1: Fuzzy business vision for Enterprise Integration (Business risk). The CTO, or equivalent in a leadership position, fails to provide a compelling vision of business with EI versus business without EI; the business scenarios that integration would enable, such as shorter processing cycles, reduction in rework or ability to provide real-time information, are not well-communicated. The business objectives that integration is meant to serve remain shrouded, so the project becomes perceived as an IT 'techie' project rather than one motivated out of business necessity.

***RMP:** Pinpoint problem areas in current business and identify opportunities not capitalized; articulate measurable business objectives; walk-through high-level business scenarios, and hold round-table session with senior executives.*

RA-S2: Lack of business stakeholder buy-in and support for the EI project (Business and organizational risk). The stakeholders on the project (individual business units, IT departments, and external organisations) do not fully buy-in to the project. This lack of commitment may be due to internal politics, or stakeholders being overly protective about their IT systems and data without seeing the bigger picture and benefits that an integrated solution would bring. On large EI projects involving multiple business units, an EI solution may be of a higher business priority for one business unit than for another business unit. This asymmetry leads to a situation where full project commitment is not mutually shared across all stakeholders. In large organizations, business units are increasing autonomous and business and IT budgets are locally rather than centrally managed. In some cases, there is no lack of stakeholder buy-in for the business rationale for the EI project, but issues such as how project costs and resources are allocated can become significant impediments that, if not addressed, eventually lead to stakeholder disillusionment.

***RMP:** Articulate win-win benefits; emphasize mutual goals; establish steering authority with representation from stakeholders; create joint project teams; include stakeholders in formal sign-off processes.*

RA-S3: Poorly-written business case for integration with lack of clear ROI (business risk). The business case fails to articulate the full business benefits that EI would deliver. The measures used to construct a business case depend upon the goals and objectives of the specific project. On an EI project where the goal is to reduce processing cycles or improve process efficiency, measures such as cost savings per transaction, for example, would be appropriate. On an EI project where the goals are revenue driven, measures such as revenue and profit are appropriate. On an EI project where the objective is to improve customer service, measures such as customer retention and customer satisfaction are relevant. In many cases, such measures, which would substantiate a ROI calculation, are stated vaguely or not at all.

Another issue in preparing the business case is calculating the total cost of ownership (TCO) of an EI solution. Doing so requires an understanding of the different architectures that can be used to create an EI solution. Solutions can range from an EI package from an integration vendor to developing point-to-point interfaces between individual systems. A TCO calculation should include at least the following components:

- technical infrastructure,
- adapter acquisition or development,
- re-engineering or extension to existing legacy systems,
- maintenance and operations, and
- consultancy and training.

Inexperience with EI projects can lead to unrealistic assumptions about TCO. Furthermore, a lack of clear ROI is common on longer-term EI projects that span over 12 months where business conditions can change rapidly during the project. Consequently, the EI project is rejected altogether or eventually dies from a lack of genuine management and stakeholder support.

RMP: *Identify key measures of success; provide realistic and well-grounded ROI; break long integration projects into stages with interim deliverables; provide total cost of ownership for integration solution and compare against business cost of non-implementation.*

RA-S4: Lack of a full and thorough assessment of the organizational impact of the EI solution (organizational risk). A new EI solution often causes changes to existing organizational structures, the creation of new organizational structures, and changes to the roles and responsibilities of employees. The need for employees to develop new skills or familiarize themselves with new working practices places demands on training, personal development, and manpower planning. Organizations often fail to understand the full organizational implications of a new EI solution until it is too late. This lack of organizational readiness is often the cause of delays to the 'live' release of an EI solution.

RMP: *Identify key project stakeholders; understand impact to each stakeholder group in terms of changes to working practice; reassess roles and responsibilities; create a plan for organizational readiness.*

RISK MANAGEMENT IN THE PLANNING PHASE

RA-P1: Business requirements not fully understood (business risk). Business requirements pertaining to the EI solution are not fully understood at the outset. This lack of understanding may be the result of a large conceptual gap between the business vision and the specific business functionality that needs to be specified. The business stakeholders may have yet to fully think through the fine details of their requirements, work through the business implications of the EI solution, or may need specific guidance from technical teams as to which particular area needs clarification. Either way, the technical team is left with a partial rather than complete understanding of the business requirements which, if left unattended, will lead to the implementation of solutions that do not fully meet business needs.

RMP: *Identify business stakeholders; understand existing business practices, processes and workflow; highlight business problems; model business processes and workflows; capture and document business requirements; build prototypes; conduct demos or walkthroughs.*

RA-P2: Lack of project synchronization and timing (business and organizational risk). Though individual stakeholders agree on the overall business need for EI, issues of priorities, timing and budgeting cycles can act as impediments to developing a coherent and feasible project plan. It is not uncharacteristic, for example, for business stakeholders to make urgent and immediate demands for an EI solution to technical stakeholders with a lengthy backlog of existing IT projects to complete. Different business units may also differ in the way budgets are created and allocated. Where an EI project involves the 'pooling' of budgets from different stakeholders, obtaining timely commitment to project funding and resources can be problematic.

RMP: *Understand priorities and resource commitments required from each stakeholder; plan early ahead of budgeting decisions; create a resource plan that identifies when resources will actually be required; get written commitment for resource and budget allocation.*

RA-P3: Unrealistic estimation of integration work activities (technical risk). Project estimation is based purely on guesswork without reference to previous integration projects or application of a methodical estimation approach. Consequently, scheduled work activities take longer than planned, which is frequently the case with development of custom adapters, wrappers, or new interfaces. In addition, unanticipated activities emerge during the course of the project, such as when a vendor's integration products do not work as expected in the target environment.

RMP: *Estimate analysis work on scope of business process, interface definition and business interactions; estimate development work based on number of adapters, interfaces and extension applications, and on complexity of each; where previous data exists, estimate based on analogy with similar projects.*

RA-P4: Integration scope creep (technical risk). New integration requirements creep into the project, either due to a lack of clarity in the original requirements, delayed injection of new requirements, or due to weak controls in the requirements management process. Typical areas of scope creep include additional business processes or hidden complexity within existing business interactions. What may start out as a well-bounded and achievable project becomes bloated and over-stretched.

RMP: *Enforce requirements management process with impact analysis and formal sign-off; highlight requirements that are explicitly excluded; establish release management controls where new requirements are gradually introduced with subsequent releases of the integration solution; ensure business process, adapters, interfaces and all other integration components are clearly specified.*

RA-P5: Project silos resulting from lack of an overall integration architecture and enforced standards (technical risk). Because an enterprise view of the integration architecture is lacking, individual integration projects become silos with localised standards and a project-specific mix of integration technologies and platforms. For example, one project that standardises on a centralised hub-and-spoke messaging architecture whilst another on a decentralised bus-based architecture. While individual project integration goals may be met, future gains from having an enterprise-wide integration architecture are made more difficult to achieve.

RMP: *Understand high-level integration requirements to delineate perimeter of the holistic integration solution; define enterprise-wide integration architecture as reference point for standards; validate project-specific architectures against enterprise-wide integration architecture.*

RA-P6: Shortfall in integration skills and expertise resulting in wrong technical decisions (technical and organizational risk). Integration is an endeavour that requires specialist knowledge and expertise. The project attempts to tackle complex architectural or implementation work without the necessary skills onboard, e.g. custom adapter development or messaging infrastructure design. Non-optimal decisions are made, and the project becomes plagued by technical hitches.

RMP: *Identify skill gaps; engage external consultants for higher valued activities such as strategic integration architecture design and where there are specific skills gaps; negotiate combined product purchase and consultancy packages with vendors; outsource well-defined packages of integration work.*

RA-P7: Integration 'out-of-the-box' mentality (technical risk). Slick vendor marketing gives the impression that integration can be achieved 'out of the box' by buying an off-the-shelf integration solution and plugging it into an organisation's existing IT architecture. The real, dirty work of adapter creation, legacy system extension, and interfacing is hidden behind the marketing veneer, but becomes painfully apparent during the course of the project. Work that was never anticipated now becomes a reality, with significant implications on project resources and schedules.

RMP: *Thoroughly evaluate packaged integration solutions offered by vendors; obtain independent expert opinion and analysis; check availability of adapters for existing IT applications, particularly non-popular packaged applications; shift onus on vendor to deliver a solution rather than on simply selling a product.*

RA-P8: Ignoring business process management and jumping straight into technology integration (business and technical risk). The project becomes blinkered by technology integration goals, e.g. connecting system A to system B using XML. Integrated business processes, the true drivers and context for integration, either are ignored, forgotten or lost in the short-term-ism of technology integration. As a result, although systems are integrated, little business value emerges, leading many to question the rationale for integration in the first place. Several underlying factors can contribute to this type of risk.

- A lack of overall understanding of the relationship between business process and technology integration. Individuals need to understand both areas, and be able to bridge this gap. Unfortunately, individuals which such knowledge can be difficult to find.

- Business processes are often constrained by the technology itself. Individuals are steered by what the technology can achieve rather than the reverse. As a consequence, technology becomes the focal point, and the central activity of business process modeling becomes a secondary concern.

RMP: *Derive integration requirements from business process needs; ensure traceability between process needs, integration requirements and design components of the integration solution; assess new technical requirements against relevance to business process.*

RA-P9: Adopting a 'single supplier' strategy rather than going 'best-of-breed' (technical risk). The organisation chooses to buy applications from a single vendor in the mistaken belief that integration will be easier. In reality, inflexibility and shortfalls in the integration technology provided by a single supplier becomes an architectural liability that compromises the original requirements.

RMP: *Establish integration needs; identify all possible solutions, including both single supplier and best of breed solutions; study integration tools and facilities provided within each solution; evaluate possible solutions against integration needs.*

RA-P10: Ill-defined organizational structure and roles (organizational risk). It is not clear who is meant to oversee or handle new processes arising out of changes to working practices. Typically, the responsibilities are either assumed to pertain to an existing workgroup but without clear and explicit communication being made, or were not anticipated in the first place due to weaknesses in pre-training or the organizational impact assessment. The confusion, if left unresolved, can lead to detrimental effects on customer service levels.

RMP: *Walkthrough new business processes expected after EI solution implementation; identify changes in working practices; revise roles and responsibilities accordingly; delineate lines of communication and reporting; communicate to workers through training sessions.*

RISK MANAGEMENT IN THE IMPLEMENTATION PHASE

RA-I1: Lack of an agreed, well-defined end-to-end business process model (business and technical risk). The business stakeholders fail to define and agree on an end-to-end business process model that is sufficiently comprehensive to drive through the implementation of an integration solution. Business rules remain fuzzy, or even worse, are missing altogether. Consequently, business process modelling is not completed until late in the implementation phase, causing unnecessary delay to the overall delivery schedule.

RMP: *Conduct business process analysis and modelling early during the implementation phase; seek formal agreement and approval from business stakeholders before major design work takes place.*

RA-I2: Semantic mismatch of data and lack of an agreed information model (technical risk). The data that is shared between two or more applications is not semantically consistent. Data attributes in one application are interpreted differently by another application. For example, delivery date could be interpreted in one application as the delivery date as requested by the customer, and interpreted in another application as the actual delivery date. The lack of a semantically agreed information model becomes the main cause of behavioural irregularities.

RMP: *Clarify the meaning of business terms used; agree on a common information model or at least cross reference terms which are semantically equivalent.*

RA-I3: Use of proprietary, rather than open standards (technical risk). Proprietary protocols and data formats are chosen over open standards on the justification that the organization's problem is 'special and unique' or that open standards would be prohibitively expensive or take too long to implement. While short-term gains are achieved with proprietary standards, the case for open standards becomes stronger over time, and the organization is left with a significant re-engineering effort.

RMP: *Consider future, as well as current integration requirements; relate future integration plans to long-term business plans; conduct cost-benefit analysis for open standards including cost of not using open standards such as lost business opportunities.*

RA-I4: Performance issues with the integration solution (technical risk). The integration solution suffers from performance problems and is unable to meet Quality-of-Service (QoS) requirements in terms of response times, load handling or throughput. This outcome may result from factors related to adapter design, synchronous communications, translation between data formats, or the messaging infrastructure. Even worse, because performance issues are identified late on in the project, the effort required to fix performance issues significantly delays the project delivery schedule.

RMP: *Conduct feasibility studies to identify performance issues and validate proposed performance solutions; conduct stress and load testing early on in the integration project lifecycle and subsequently at regular points during the lifecycle.*

RA-I5: Dangerous convergence towards point-to-point integration (technical risk). Point-to-point integration, where an individual IT system is directly integrated with another system, is used in situations where broker-based architectures are more appropriate, such as in B2B and EAI scenarios where there are M:N relationships between IT systems. Over time, 'spaghetti' integration emerges, resulting in a non-scalable architecture where adding another IT system becomes increasingly troublesome. The architecture becomes less flexible to business change and maintenance costs are high.

RMP: *Establish high-level integration architecture as a framework for designing integration solutions; define conditions under which to consider point-to-point versus broker-based architectures; conduct technical review and approval process for integration designs.*

RA-I6: Sprawling of business logic across integration architecture (technical risk). The business logic that define routing, data-transformation and other rules are sprawled across the integration architecture. No consistent policy governs whether business logic should be centralized or decentralized. A major maintenance problem arises not only because business logic is difficult to locate, but because portions of business logic become embedded and 'hard-wired' within applications or adapters, making changes impossible without re-coding.

RMP: *Ensure routing and data-transformation logic are explicitly defined; establish consistent policy on logic centralization/decentralization; capture rules in a database or configuration files for ease of future change.*

RA-I7: Use of immature technologies and products that are not ready for business-critical solutions (technical risk). The project attempts to 'over-innovate' and use new technologies such as Web Services and early versions of vendor products in business-critical integration solutions. While persuasive 'on paper', the technologies and products lack an established track-record, the immaturity of which manifests itself in technical bugs that eventually prove insurmountable. Significant re-architecting ensues, causing excessive project backtracking and delay.

RMP: *Closely monitor technology developments; plan and conduct significant feasibility and proof-of-concept testing as part of formal project plan; use feasibility testing as gate for go-no-go technology decisions; request for and follow-up references from vendors on successful implementations of their products; use newsgroups and the Web to discover actual case-study experience with vendor products.*

RA-I8: Restricted functionality in APIs provided in applications and integration tools (technical risk). Application packages and integration tools claim their APIs offer an easy and effortless path to integration. On closer examination, however, the APIs are restricted in functionality, severely limiting their actual usefulness to fully deliver against business requirements.

RMP: *Understand functional requirements of integration solution; map functional requirements against functionality provided within API; conduct proof-of-concept testing on required functionality.*

RA-I9: Loss of data integrity through integration directly at the data, rather than application, level (technical risk). The integration strategy is overly focussed on database synchronization and replication, rather than via the applications that are meant to control access to databases. As data maintenance errors occur, the logical data model is broken and data integrity is lost. Depending upon the severity of the loss of integrity, the organization is left with the choice of living with the consequences of inconsistent information or conducting a major data cleansing exercise.

RMP: *Eliminate or minimize direct access and update of information in databases; protect data integrity through applications that interface with the database.*

RA-I10: Failing to design end-to-end security within the integration solution (technical risk). Security is applied inconsistently and in piecemeal fashion between different points within the integration solution, resulting in gaps in the overall end-to-end security solution. For example, messages sent between IT systems may be encrypted, but individual applications must have the ability to decrypt such messages securely. Security loopholes necessitate significant re-engineering of the existing integration architecture.

RMP: *Identify end-to-end security requirements; identify processing that takes place across the public Internet and that which occurs within the organisation's network; encrypt sensitive information; in B2B scenarios where non-repudiation is a factor, authenticate based on certificates or tokens rather than just username and password; ensure design of security solution covers end-to-end business process.*

RA-I11: Over-complicating the extension of legacy IT systems (technical). Programmatic approaches to extending legacy IT systems based on the use of complicated APIs are used in situations where simpler 'screen-scraping' approaches would have sufficed. In some cases, parts of the legacy system are written. As APIs are intrusive in nature, the development path becomes more complex both technically and in terms of overall planning of design, test, rollout, and cutover activities.

RMP: *Understand current and anticipated legacy system integration requirements; for business-critical legacy systems, chose non-intrusive integration approaches where possible; avoid programmatic approaches to legacy IT extension unless requirements can not be met by simpler approaches.*

RA-I12: Business launch plans not well thought-out or communicated (business and technical). In many cases, the launch of an online product or service is dependent upon the completion of EI work. Business launch plans can place certain demands on the EI solution in terms of technical readiness. For example, the need to run a pilot system for an initial period of time or to have demonstration accounts active. Particularly in the case of e-business and B2C commerce, the execution of marketing plans and promotions can drive unusually high volumes to a Web-site. Without a well communicated business launch plan, and analysis of the impact of the launch plan on the EI solution, there is a danger that the EI solution may not be ready to fulfill those launch plans.

***RMP:** Understand business launch activities; identify timescales and dates of business launch activities; assess implications of business launch on EI solution and resources; relate technical goals to business launch goals and resolve any conflicts.*

RA-I13: Change management plans not prepared (business and organizational risk). The introduction of a new EI solution is normally accompanied by changes to existing working practices. In many cases, fresh business policies need to be formulated, new business processes operationalized, escalation and reporting channels defined, relevant training programmes implemented and new workplans established. Delays in any of these change management areas can impact business readiness, even though the EI solution may be in a state of technical readiness.

***RMP:** Define new business processes and working practices; define emergency 'manual' procedures; relate processes to organizational structures; clarify reporting and escalation channels, assess resourcing requirements and relevant training requirements; formulate change management plan; relate change management plan to business launch and technical milestones.*

RISK MANAGEMENT IN THE ROLLOUT PHASE

RA-R1: Release plan overly focussed on 'low value' integration (business risk). The release plan that describes the rollout strategy for the integration solution is overly focussed on low-value integration projects that offer limited business value. Business stakeholders and senior management do not see early ROI, and begin to call into question the business value that integration was meant to deliver in the first place.

***RMP:** Conduct scenario planning as a way of managing expectations of business holders and senior management; include some 'quick-wins' early on in the release plan to gain management confidence; shape the release plan around business priorities.*

RA-R2: Absence of comprehensive transition and migration plans (technical and organizational risk). The organization lacks sound transition plans for migration from the 'old' IT solution to the new EI solution. Such plans serve a purpose of minimizing system downtime, keeping the business operational, and facilitating the introduction of new technology. The effect of poor transition and migration plans can be seen in a failure to successfully cut-over from an old to new IT systems, and the inability to roll-back to the pre-cutover state. Both of these outcomes can leave an organization stranded in a precarious state where they may be unsupported by business-critical integration. Part of the difficulty lies in the fact that it is hard to anticipate all the things that need to be addressed in the transition plan. Simulated or 'practice' transition and migration plans can be a poor substitute for the real thing. In addition, the organizational mobilization and co-ordination needed to manage the transition from start to finish can be a significant exercise in itself, particularly in cases where the end-to-end 'length' of a transaction passes through many points.

***RMP:** Identify cutover and transition activities; identify rollback approach; formulate transition plan; test transition and migration plans; create early walk-through scenarios prior to system release.*

RA-R3: Software upgrades cause adapter or integration component failure (technical risk). Upgrading software applications to new versions causes existing adapters or other integration components either to behave incorrectly or to stop working altogether. Even worse, the necessary upgraded adapters are not immediately available with new versions of software, leading to dilemmas about what and when to upgrade.

RMP: *Obtain vendor assurance that upgrades are compatible with the existing environment; institute strict testing process before releasing upgrades into the production environment; automate regression testing so that upgrade testing can be performed swiftly and with minimum effort; define upgrade plan.*

RA-R4: Lack of flexibility in accommodating new business requirements (business and technical risk). The integration solution, once installed, proves inflexible in accommodating new business requirements. Changes to the business process that should have been effortless to implement become major headaches on a change list that cannot be executed without first carrying out extensive impact analysis. One common cause is an excessively tightly-coupled integration architecture, where routing, data transformation, and workflow logic becomes hard-coded within the architecture itself, inadvertently introducing dependencies between IT applications, adapters, data transformation, workflow applications and other integration components.

RMP: *Drive technical integration solution forward from the business process model; ensure business rules are not 'hard-coded' into the integration architecture but explicitly factored out into a database or configuration files; ensure technical and messaging services are established at a sufficiently fine level of granularity rather than as a large monolithic service.*

RA-R5: Lack of EI evaluation (business). Business objectives associated with EI solutions are often related to improved customer service, process efficiency, faster turnaround, and access to real-time information. However, after the EI solution is implemented, the effectiveness of the EI solution is not (or hardly) evaluated in accordance with its business objectives. Once possible reason for this state of affairs is that the precise business objectives were not crystallized in the first instance, and so any formal evaluation is difficult. Another possible reason is fear of admission of failure. Given that a project represents sunk costs, people are reticent to label the project as less than successful. The lack of formal evaluation can suppress worthwhile debate about possible improvements that could be made to the EI solution. The end result is an EI solution that, while it may be contributing to the business, may be doing so sub-optimally.

RMP: *Crystallize business objectives and goals; conduct formal evaluation of EI solution with business stakeholders; identify and document improvements; use improvements to drive release plan.*

RA-R6: Apparent lack of EI governance structure (business and organization). IT governance encompasses the organization structures, policies, practices and procedures for responsibly managing IT and information resources within an organization. One problem related to EI projects is a lack of clear EI governance, which can often be traced back to the absence of a single owner of the EI solution. A further related issue is the lack of centralized EI governance, and absence of a central forum for making decisions about the EI solution. Both problems can manifest themselves in terms of poor utilization in IT resources, haphazard maintenance, prolonged response to handling operational issues, and lack of attention towards issues of user satisfaction.

RMP: *Define governance roles and responsibilities, ensure clear accountability; review existing IT governance or programme management structures and establish EI governance structures as necessary; define governance processes and procedures (tools such as COBIT (Lainhart 2000) might be useful); relate governance processes to operations, maintenance and release anagement processes.*

VI. SUMMARY OF FINDINGS

FRAMEWORK FOR RISK MANAGEMENT ON EI PROJECTS

As the trend towards greater connectivity and real-time processing continues, EI will become an increasingly major component in IS projects. The discussions with project managers and business managers in our study underlined the high level of complexity often inherent in EI projects, and the many different types of risks that serve as potential project pitfalls. Unless such risks are managed effectively, there will be a greater propensity for EI projects to fail. The findings from this research lead towards a proposed framework for risk management on EI projects (Fig 4)

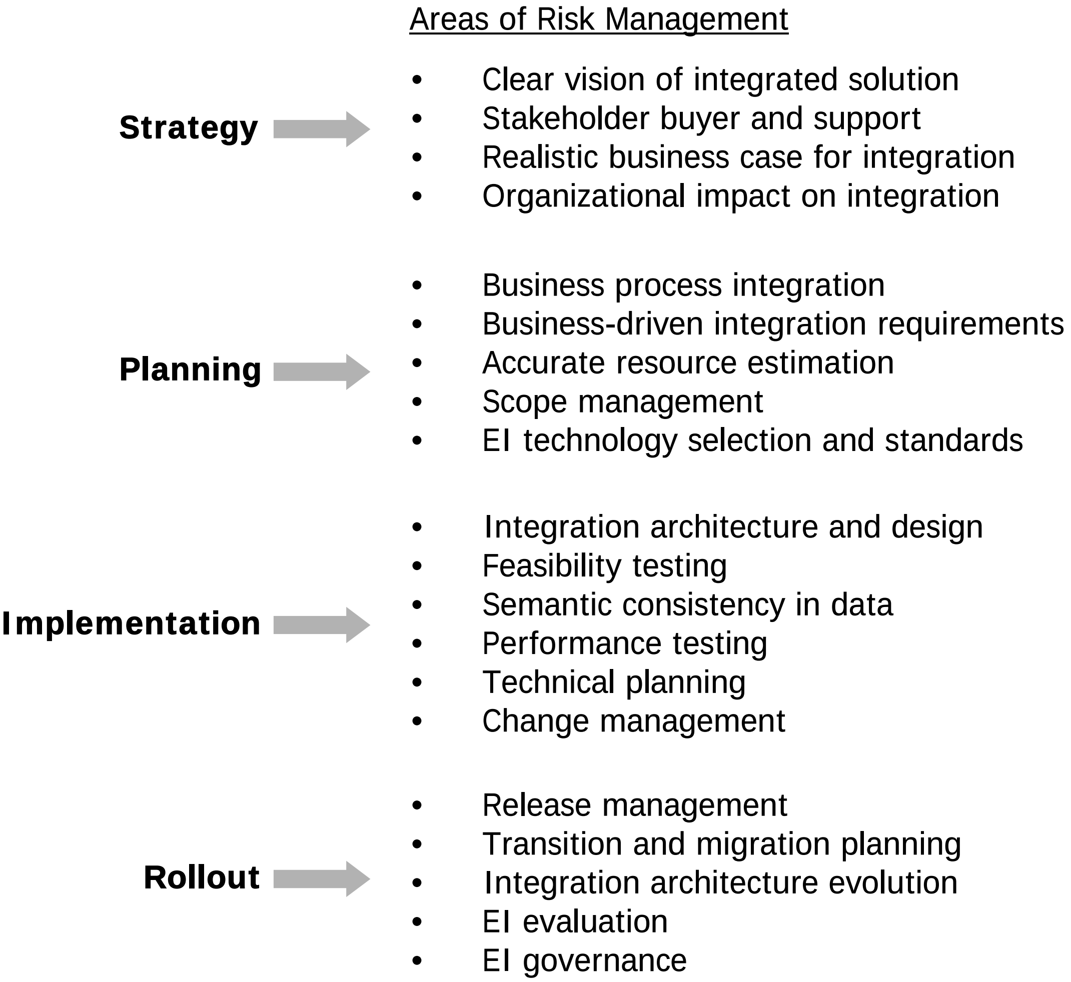

Areas of Risk Management
Strategy
• Clear vision of integrated solution
• Stakeholder buyer and support
• Realistic business case for integration
• Organizational impact on integration
Planning
• Business process integration
• Business-driven integration requirements
• Accurate resource estimation
• Scope management
• EI technology selection and standards
Implementation
• Integration architecture and design
• Feasibility testing
• Semantic consistency in data
• Performance testing
• Technical planning
• Change management
Rollout
• Release management
• Transition and migration planning
• Integration architecture evolution
• EI evaluation
• EI governance

Figure 4 Framework for Risk Management on EI projects

The framework identifies specific areas of risk management whose criticality depends on the phase of the EI project lifecycle, namely the strategy, planning, implementation, and rollout phases. Ideally, the risks in one phase must be addressed and managed before moving onto the next phase. For example, in the strategy phase, it would be dangerous not to address issues relating to a clear vision for enterprise integration before moving onto the planning phase. Our study confirmed that many areas of risk management apply equally well to conventional IS projects as they do to EI projects.

A noteworthy finding from the study was the importance of clarifying the business drivers for EI early on in a project. Without this clarification, follow-on activities in the project such as examining business processes and defining integration requirements are easily misguided and can lose focus. The cascading effect of inappropriate choices at the business level can exacerbate and amplify technical risks further into the project. For example, failure in a vision for enterprise integration to articulate the need to interoperate with new business partners in the future may lead to an integration architecture that is not extensible or easily scalable. Business and technical models must therefore be aligned with each other, and any discrepancy between the two addressed.

Another significant finding was the importance of business stakeholder buy-in and support for an EI project. Some of the ways in which stakeholder support can be demonstrated includes attendance at project meetings, reviewing and providing feedback on important project documents, releasing staff to work on the project, contributing to project resources, and participating in collaborative project activities such as business process design. However, participants in the study indicated that while gaining stakeholder support at the outset of a project was one issue, maintaining that support throughout the duration of a project was another issue. Lack of clarity in business benefits, unclear scope of EI work and resource commitment, changing priorities of the stakeholder, and poor project performance are contributing factors to a lack of, or decline in, stakeholder support.

An apparent lack of interest shown by any stakeholder obviously creates a dampening effect on the rest of the project. An essential task therefore is to clearly articulate the win-win benefits of EI to all stakeholders, and to brief them fully on the scope and nature of the work and resources required. A further question is who should take responsibility for this coordination. Normally, an IT project that offers a clear benefit to a particular business unit is championed by the business owner within that unit. EI projects, however, by their very nature, cut across multiple business units. It would therefore seem important that either an individual with overall responsibility for these business units champions or sponsors the EI project, or that the sponsors be a group of senior representatives from each business unit who are not only committed, but attach equal importance to the EI project.

The participants who participated in the study also agreed that they alone could not effectively manage the entire spectrum of risks that occurred on an EI project. Importantly, project managers relied on project members to be aware of the risks in their own area of the project and to flag these risks at any early stage. The involvement of all project members in regular risk reviews would therefore seem good project practice.

VII. CONCLUSIONS

CONTRIBUTIONS AND POST-ANALYSIS

The contributions made in this paper are three-fold.

1. A lifecycle model for EI projects is proposed (LEIP). Though our model is in essence a derivative of the Waterfall model, few structured methodologies to date specifically address processes around the creation of EI solutions.

2. A set of risk areas for EI projects is presented, framed within LEIP. Although risk factors for IT projects are the subject of previous work, none of this work focussed specifically on EI projects. The results from our workshop indicate that significant areas of risk specific to EI projects need to be considered over and beyond the risk associated with IT projects in general.

3. A set of Risk Management Practices (RMPs) are presented. Though the RMPs are not documented in detail, the practices go beyond what is currently available in terms of explicit risk management practices for EI projects. However, it is unavoidable that some of our RMPs represent good project practice for all IT projects, not just EI projects.

It should be noted that many of the risks identified in our study are of the same technical nature as risks found in other types of IT projects. Of the total of 33 Areas of Risk (RAs) identified, over half can be considered generic risks. Indeed, I uncovered many similar types of risk to those identified in early studies of information system failures [Ewusi-Mensah and Przasnyski 1991; Ewusi-Mensah 1997]. This finding naturally raises the question of why, given our understanding of risks, IS and IT project failure still continues to be a recurring problem. One possible reason is that risk management practices are poorly executed, if at all, and that the successful management of IS and IT project relies just as much on the ability of individual managers as it does on knowledge of risk management process and practices. This hypothesis in itself would be an interesting area for further research.

STUDY LIMITATIONS

While our study produced useful results that met the objectives and intent of the management sponsors at Firm X's TSCs, I recognize that the results of the study and the study methodology is limited in a number of ways.

- The study used a small population of 21 individuals, albeit experienced managers and architects, working across 12 separate projects. This group was sufficient to generate many ideas but hardly constitutes the basis for what can be considered a large and extensive study.

- I took few steps to validate the effectiveness of the RMPs, and propose them largely on the basis of the experiences of our target population and what made sense to them in terms of good practice. However, verifying that our RMPs represent not only good practice, but also best practice, would require further analysis of many more EI projects as well as proposing metrics that would help to substantiate any claims in risk management improvement. In parallel, this would also require us to be more specific about the details of how to implement the practices I mentioned.

- I did not link our RAs and RMPs to any specific type of EI project or other factors that distinguish one type of EI project from another. For example, some RAs or RMPs may be more relevant to B2B projects than Web integration projects. As Turner [2003] points out, it is important to identify the specific conditions under which certain practices are appropriate.

AREAS OF FURTHER RESEARCH

Future research should be directed at addressing some of the study limitations indicated in the previous subsection. Our immediate follow-on research is centred on validating the RAs and RMPs across a broader community of practising project managers and architects. However, rather than do this in the style of a facilitated workshop, I plan to take a case-study based approach which would involve observing the risk and risk management practices actually used by project managers and architects on real EI projects. This alternative approach provides a means of validating the RAs and RMPs identified in our study and will also expose how risks affect project decision-making and the course a project ultimately takes.

Discussion with individuals at the TSCs have also highlighted the problem that even though RAs and RMPs are documented, there is no little support for operationalizing this in terms of actual project practice. This concurs with research elsewhere, which has highlighted the importance of contextual factors, e.g. risk awareness and experience of projects managers, in the successful management of risk (Ropponen and Lyytinen 2000). Given the demonstrated impact of peer reviews in the software process, I are currently developing structured peer review processes for project risk management to address the issue of operationalization and developing analysis and documentation tools for supporting the peer review process.

Editor's Note: This article was received on 5-1-03 and was published on March 30, 2004. It was with the author for 8 months for three revisions.

REFERENCES

Boehm, B. W. (1989), *Software Risk Management*, Los Alamitos, CA: IEEE Computer Society Press,.

Buchanan, D. and Connor, M. (2001), "Managing Process Risk: Planning for the Booby Traps Ahead", *Strategy and Leadership*, 29(3), May-June.

Carr, M.J., Konda, S.L., Monarch, I., Ulrich, F.C. and Walker, C.F. (1993), *Taxonomy-Based Risk Identification,* Pittsburgh, PA: Software Engineering Institute, Technical Report CMU/SEI-93-TR-6, 1993.

Charette, R.N. (1989), *Software Engineering Risk Analysis and Management*, New York: McGraw-Hill

Cornford, S.L., Feather, M.S. Hicks, K.A.(2001), "DDP-a Tool for Financial Management", Aerospace Conference, 2001, IEEE Proceedings. , Volume 1 , Pp. 1/441 -1/451.

Cummins, F. (2002), *Enterprise Integration*, New York: John Wiley.

Elkington, P. and Smallman, C. (2002), "Managing Project Risks: a case-study form the utilities sector", International Journal of Project Management, 20(1),pp.49-57.

Ewusi-Mensah, K., and Przasnyski, Z. H. (1991), "On Information Systems Project Abandonment: An Exploratory Study of Organizational Practices", MISQ 15(1) , March.

Ewusi-Mensah, K. (1997), "Critical Issues in Abandoned Information Systems Development Projects", *CACM,* 40(9), September.

Gilb, T. (2002), "Risk Management: A Practical Toolkit for Identifying, Analyzing, and Coping with Risks", *Software Quality Professional*, 4(4), pp. 6 - 17, September.

Keil, M., Cule, P.E., Lyytinen, K. and Schmidt, R.C. (1998), A Framework for Identifying Software Project Risks, *Communications of the ACM,* 41(11), 1998.

Lainhart, J.W. (2000), COBIT: A Methodology for Managing and Controlling Information and Information Technology Risk and Vulnerabilities, *Journal of Information Systems,* Volume 14, 2000 Supplement, pp. 21-25.

Lam, W. and Shankararaman, V. (2004), A Methodology for Enterprise Integration Projects, IEEE IT Professional, March-April, 6(2), pp.40-48..

Linthicum, D. (2001), *B2B Application Integration*, Reading, MA: Addison Wesley.

Mawby, D. and Stupples, D. (2002), Systems Thinking for Managing Projects, *Engineering Management Conference, 2002. IEMC '02*. 2002.

McKeen, J.D. and Smith, H.A. (2002), New Developments in Practice II: Enterprise Application Integration, *Communications of the Association for Information Systems*, Volume 8:451-466.

Myerson, M. (1996), *Risk Management Processes for Software Engineering Models*, Boston, MA: Artech House Books.

Murthi, S. (2002), Preventative Risk Management for Software Projects, *IEEE IT Professional,* September/October, 2002.

Reifer, D. (2002), Ten Deadly Risks in Internet and Intranet Software Development, I*EEE Software*, March/April 2002.

Ropponen, J. and Lyytinen, K. (2000), Components of Software Development Risk: How to Address Them? A Project Manager Survey, *IEEE Transactions on Software Engineering*, 26(2), February.

Roy, G.G.; Woodings, T.L.(2000), Framework for Risk Analysis in Software Engineering, *Proceedings of the Seventh Asia-Pacific Software Engineering Conference* (APSEC-2000), Page(s): 441–445, Ruh, W.A., Maginnis, F.X. and Brown, W.J. (2001), Enterprise Application Integration, John Wiley, New York, 2001.

Sage, A.P. (1995), Risk Management Systems Engineering, *Proceedings of IEEE International Conference on Systems, Man and Cybernetics,*
Volume 2, 22-25 Oct 1995, Page(s): 1033 -1038 vol.2, 1995.

Schneier, R. and Miccolis, J. (1998), "Enterprise Risk Management", *Strategy and Leadership*, 26(2), Mar-April.

Simons, R.L. (1999), "A Note on Identifying Strategic Risk", *Harvard Business School,* 9-199-031, 1999.

Sisti, F.J. & Joseph, S. (1994), Software Risk Evaluation Method Version 1.1, , Software Engineering Institute, 1994. SEI-94-TR-019

Smith, H.A., McKeen, J.D. and Staples, D.S (2001), "Risk Management for Information Systems: Problems and Potential," *Communications of the Association for Information Systems*, Volume 7, Article 13, 2001.

Sumner, M. (2000), Risk Factors in Enterprise-Wide/ERP projects, *Journal of Information Technology*, 15:317-327.

Turner, R. (2003), "Seven Pitfalls to Avoid the Hunt for Best Practices,: *IEEE Software*, Jan/Feb.

Weatherall, A. and Hailstones, F. (2002), "Risk Identification and Analysis Using a Group Decision Support Systems (GSS)," *Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS-35),* January 07 - 10, 2002, Big Island, Hawaii.

Whittaker, B. (1999), "What Went Wrong? Unsuccessful Information Technology Projects," *Information Management & Computer Security*, 7(1), 1999.

Wright, S. and Wright, A.M. (2002), "Information System Assurance for Enterprise Resource Planning Systems: Unique Risk Considerations", *Journal of Information Systems*, Vol 16, 2002 Supplement, pp. 99-113.

Zsidisin, G. A. (2003), "Managerial Perceptions of Supply Risk", Journal of Supply Chain Management, 39(1), pp. 14-24.

GLOSSARY OF ABBREVIATIONS

API application programming interface—A set of programmatic functions through which an application makes its functionality available to other external applications.

B2C business-to-consumer commerce—A business that offers products or provides services directly to consumers.

B2B business-to-business commerce—A business that offers products or provides services to other businesses.

CICS customer information control system—A transaction processing application produced by IBM that is commonly used on mainframe computing platforms.

COBIT control objectives for information and related technology—A process model developed to assist organizations with the management of information technology resources particularly in relation to security and control. COBIT provides tools that enable an organization to measure and assess their performance against stated control objectives.

CTO chief technology officer—An individual charged with the responsibility for managing technology within an organization.

CRM customer relationship management— Aligning a organization's people, processes and technology in such a way as to create a customer centric organisation that enhances customer interactions.

EAI enterprise application integration—The integration of IT systems within an enterprise, typically to improve business efficiency and to meet the needs for real-time information processing.

EDI electronic data interchange—A standard format for data exchange between trading partners that is particularly well-adopted in the retail, manufacturing and transportation industry sectors.

EI enterprise integration—A general term that refers to the integration of IT systems and business processes both within the enterprise and between different enterprises.

ERP enterprise resource planning—An integrated suite of module-based packaged applications, typically from a single vendor, that handles a diverse range of enterprise functions such as inventory management, accounting and human resource management.

MOM message-oriented middleware—The integration of applications based on the exchange of messages between applications via a specially designed fault-tolerant messaging infrastructure.

MVS multiple virtual storage—An operating system produced by IBM that is installed on many of its mainframe computers.

QoS quality of service—Measurable requirements that relate to the characteristics of a particular service which are relevant to users of the service such as responsiveness and availability.

ROI return on investment—The value that is expected to be derived from an undertaking in relation to the costs associated with that undertaking. A ROI calculation is normally performed as part of a business case or IT justification.

SCM supply chain management—The co-ordination, optimization and integration of materials and information flow as they move through the supply chain from supplier to the eventual consumer.

TCO total cost of ownership—A final figure that reflects both the direct and indirect costs associated with the purchase, maintenance and support of a product or service.

XML extensible markup language—A flexible means by which information can be described in a format that can be shared with and understood by other applications.

ABOUT THE AUTHOR

Wing Lam is a member of the faculty at Universitas 21 Global, an online business school established from 16 member universities in the Universitas 21 network. He is the author of over 60 journal articles and conference papers. He held academic positions and consulting positions in several large IT firms. His interests are in large-scale enterprise integration.

Communications of the Association for Information Systems

ISSN: 1529-3181