

Understanding enterprise integration project risks: A focus group study

Sandeep Puroo, Ph.D.
Penn State University,
University Park, PA. USA
Email:sandeep-
puroo@psu.edu

Sharoda Paul
Penn State University,
University Park, PA. USA
Email:sandeep-
puroo@psu.edu

Steven Smith
AccuWeather, Inc., State
College, PA. USA

Abstract

The prerequisites of success and reasons for failure for enterprise integration projects are still not well-understood as evidenced by large failure rates, including cost or schedule overruns, abandoned projects, and projects delivered with diminished functionality [37, 10]. These failures point to the inherently human activities of planning and overseeing that are critical to successful large-scale integration. In spite of a rich stream of research on systems development risks, few research efforts have attempted to understand enterprise integration risks [36]. This paper reports preliminary findings, based on an analysis of data gathered via focus groups at an organization poised to embark on an integration project, about how organizational participants perceive these risks. The analysis shows that risk perception is fuzzy, it differs significantly across organizational actors, and points to considerable information asymmetry between risk managers and project participants.

1. Introduction

A key characteristic of next-generation information systems is their ability to tie-together software services and work practices across functional and organizational boundaries. Technological feasibility for such integration has been established with alternatives such as middleware and service-oriented architectures. Organizations are making integration a high priority (CIOs consistently rank integration highly in IT spending [17]). The vision of building and deploying such integrated solutions, however, relies on human efforts to conceive of, direct and oversee large-scale integration projects. The track record for these projects has been dismal. A disturbingly large fraction of these projects has been known to incur cost overruns, run beyond expected timelines, abandoned, delivered with

limited functionality or curtailed significantly [37, 10]. From the few cases reported in trade press, we can surmise that consequences of failure tend to be crippling for the organization (e.g. [11,30]). Surprisingly, the prerequisites of success and reasons for failure for integration projects are still not well-understood [36, 6] due at least in part to the code of silence among practitioners of the craft. If systems development failures (e.g. [40]) provide an indication of the resources wasted (as much as \$250 billion), these larger systems integration projects present an even more important domain to investigate and improve risk management practices. This paper reports the results of a study - involving focus groups, carried out at an organization poised to start an integration project - that was carried out to further our understanding of key enterprise integration risks.

2. Background and Prior Research

Enterprise integration refers to the efforts undertaken by one or more organizations to achieve cross-functional integration of its information, processing and work practices. It is inherently a complex process that requires connecting hardware, operating systems, programming languages, database structures, applications, and employees. Technologies used in enterprise-wide integration projects may be classified along a continuum, where the extremes are marked as top-down and bottom-up [24]. The first refers to customization and implementation of enterprise-wide ERP software packages, whereas the second refers to utilizing solutions such as middleware products (e.g. messaging, distributed objects) to connect legacy applications that may be spread across different functional areas. The few accounts of enterprise integration efforts in the industry that have appeared in the academic literature are peppered with anecdotal accounts of events during the implementation process (e.g. [34, 36, 37]).

The general concern of risk has, however, not received much attention in this context. Instead, studies related to risks are more readily available for systems development (see, e.g. [27, 2]). In that stream, software risk is defined as a particular aspect of a development task, process, or environment, which, if ignored, will increase the likelihood of project failure [27]. A number of approaches have been devised to assess risk, including quantitative (e.g. probability of unsatisfactory events multiplied by the loss associated with their outcome) and qualitative (referring to the uncertainty surrounding the project and the magnitude of potential loss associated with project failure) [3]. Risk management approaches have been developed to identify, analyze, and tackle project portfolio risks [14], systems development risks [3-5, 9, 13, 16, 22, 32, 33, 35], requirements risks [7, 12], or implementation risks [1, 20, 23, 25, 26]. Four different approaches have been identified to address risk items, resolution actions, and heuristics (see [27]). The first approach, 'risk lists,' prioritizes risk items and helps a project manager focus on possible sources of risk [3, 32, 22, 35]. The second, called 'risk-action lists,' contains generic risk items, often prioritized, each with possible risk resolution action(s). Compared to the first approach, such lists require additional knowledge of the potential effects of different types of actions [1, 5, 19, 33]. The third, called 'risk-strategy models,' represents an instance of contingency models that relate a project's risk profile to an overall strategy for addressing it. It combines comprehensive lists of risk items and resolution actions with abstract categories of risks (to arrive at a risk profile) and abstract categories of actions (to arrive at an overall risk strategy) [22, 13]. The final approach, called 'risk-strategy analysis,' is similar to the third, but uses different heuristics. It does not link aggregate risk items to aggregate resolution actions. Instead, it adopts a stepwise analysis in which the involved actors link risks to actions to develop an overall risk strategy i.e. there is a looser coupling between the aggregate risk items and aggregate resolution actions making it more difficult to use and equally difficult to build [12, 28].

Risk management for enterprise integration projects has received little direct attention in prior work in spite of the recognition of its considerably larger scale and scope. It has been acknowledged that enterprise integration projects are more complex, and due to their distributed nature, may present multiple points of failure. With the exception of Sumner [38], who suggests an extensive list of risk items for enterprise integration projects, these risks have not been systematically investigated. Scott and Vessey [36]

suggest another model that outlines multiple categories for risks, including (a) external business context, (b) organizational context, (c) information systems context, and (d) systems implementation project context. Their analysis, which is based on two in-depth case studies (Dow Corning and FoxMeyer) presents the most comprehensive categorization of enterprise integration risks to-date, and therefore, forms the basis of some of the analysis we present in this paper.

3. Research Method

The setting for this study, which was carried out to understand perception of enterprise integration risks, was AccuWeather, Inc. a medium-sized company located in State College, PA. Three focus groups, each lasting about two hours, were conducted at the company over a period of three months. Focus groups are a qualitative research technique that relies on interaction within the group to gather data, based on topics that are supplied by the researcher, who typically takes the role of the moderator [31]. The first focus group consisted primarily of senior managers at AccuWeather. This group mainly focused on project management issues, inability of the new system to integrate business processes and inadequate success measures. The second focus group, conducted two months later, consisted mainly of users. Issues raised in this group related to staffing, user training and management direction and involvement. The third focus group, conducted on after another week, consisted of IT team members. Here, the discussion centered on technology-related issues such as hardware and software failure and failure to meet implementation timeline or requirements.

The procedure followed for each group was similar. The facilitator defined 'risk' and 'enterprise integration,' and steered the discussion, if needed, to focus on risks. The group discussed two questions: (a) What are the key risks involved in integrating information systems within your organization? and (b) What approaches may be adopted to resolve these risks within your organization?

The participants were asked to record their responses on Post-It™ notes, which were periodically posted on a whiteboard. Upon reaching a predetermined time, the notes posted by everyone were open to inspection and debate by the group. Because the notes did not bear any names, it was possible for the participants to critically examine the results during this phase. For instance, risk elements recorded during the first phase titled 'data cleansing' and 'ensuring information to be integrated is clean' may be merged

during this phase. The participants were asked to group the notes into categories during this phase. Figure 1 shows examples of focus group sessions in-progress.



Figure 1. Examples of focus groups in-session

Data collected during the focus groups included audio recordings, extensive notes, and visual records such as pictures of whiteboards. With multiple participants, each walking around the room when interacting with the whiteboard, the audio-tape recordings were not efficient, and therefore, not directly used for analysis. Instead, they provided a source that could supplement the analyses, which focused on elements and categories identified by the participants, and notes captured by the researchers. The data was cleansed by removing inconsistencies, rewording phrases for clarity and to ensure confidentiality of participants. These provided the basis for the analysis we report next.

4. Selected Findings and Analyses

4.1. Non-specificity of perceived risks

The first finding related to non-specificity of perceived risks. The focus group participants perceived risks through several broad phrases such as ‘poor planning’ and ‘data loss’ though drill-downs to specific ways of measuring the risks were largely absent during discussion. It is possible that the focus group approach did not allow reaching the required level of depth. In at least one focus group (with the users), the discussion among participants lead to what the researchers termed an ‘a-ha’ realization of the scale and complexity of the project and consequently, recognition of the seriousness of risks. This prompted the focus group to repeatedly bring up the need for management to pay attention to and manage risks. On the other hand, another focus group (with the management) exhibited

confidence in the planning that had already gone into the project, and appeared more certain of the eventual outcome of the project though they were reluctant to describe in significant detail specific elements of the project plan. All three groups, to varying degrees, did acknowledge the “socio-technical” nature of the integration project but did not attribute any specific risk elements as a result of this characterization.

4.2. Focus on internal risks

The results were further analyzed to understand whether the focus group participants identified risks that could be mapped to the four categories identified by Scott and Vessey [36]. Their study, based on an *ex post facto* analysis, showed that enterprise integration projects faced four kinds or risks: external business context, organizational context, information systems context and the project context. AccuWeather, on the other hand, was poised to embark on an integration project. Table 1 shows a simple count of risk elements in each category, identified by each focus group.

Table 1. Mapping risks elements to categories

Risk Category	Managers	Users	Developers	Total
External business context	1	0	1	2
Organizational context	3	4	0	7
Information systems context	3	1	6	10
Project context	7	2	1	10
	14	7	8	29

The data showed that the focus group dominated by management identified many more risk elements than the other two focus groups, i.e. they were more aware of risks than the other project participants. As expected, users identified more organizational context risks; developers identified more information systems risks; and managers identified more risks that belonged to the project context. It is telling that overall, the groups were focused on internal (information systems and project) risks, and less on the external business or organizational context. In light of Scott and Vessey’s [36] assessment that organizational factors are more important for enterprise integration projects, this early perception of risks provides a cause for concern.

4.3. Pre-occupation with implementation

A second form of analysis was performed to understand project stages where focus group participants attributed risks. Four broad project phases were identified: planning, design, implementation and an operational. The last stage was dictated by the data gathered, i.e. focus group participants identified risk elements that were clearly aimed at what might happen after the integration project is implemented and rolled out in the organization. Table 2 shows the results. The discrepancy (total number of elements across the two tables) is due to the fact that several risk elements were applicable to multiple project phases.

Table 2. Mapping risks elements to project phases

Project phase	Managers	Users	Developers	Total
Planning phase	6	1	1	8
Design phase	3	2	1	6
Implementation phase	5	4	7	16
Operational phase	3	4	2	9
	17	11	11	39

The data shows that a large number of risk elements were identified for the implementation phase. Interestingly, the design phase had the fewest number of risks identified, even by the developers, who were concerned largely with implementation. This possible anomaly points to the need to develop metrics and design techniques/practices that may be directly tied to the implementation phase. Pre-occupation with the implementation phase may also betray lack of research or guidelines that practitioners may use to plan for, structure, and track enterprise integration projects including simple metrics such as project completion.

4.4. Varying responses to risk elements

The risk elements summarized above were analyzed to understand how the different stakeholders interpreted these. A representative example was the risk element ‘changes in business processes.’ This was perceived by one focus group (management) as ‘lack of training’ that would be necessary. The same element was perceived by the second focus group (users) as ‘fear of attrition,’ i.e. possible loss of job function or status in the organization. The third group (developers) perceived it as ‘lack of defined processes’ that could hamper design or implementation efforts during integration. This clearly showed the multi-faceted nature of enterprise integration risks and highlighted

the need to track multiple measures (from different stakeholders) to effectively monitor overall progress.

Several other analyses were performed including attempting to understand specific risk elements, mapping specific resolution strategies to risk elements, and mapping risk elements against possible tracking mechanisms. These are not included in the paper due to space constraints but may be discussed at the workshop.

5. Recap and next steps

The study reported in this paper is one of two that were carried out simultaneously [29]. Comparative analysis of data is currently underway and will lend further richness to our analyses. Both organizations have initiated the integration projects and are proceeding with design and implementation. The data reported in this paper reflects risks perceived by organizational participants at the outset of the project in one organization. With the projects underway, we may return to the organization periodically to assess how risk perceptions evolve, how risk elements are tracked, and which resolution strategies are used.

Based on the analysis so far, two additional perspectives appear to be appropriate for further investigation. The first builds on the idea of systemic risk, treating integration projects as radical change in high-reliability organizations [8]. Translating this notion of controlling risk in socio-technical systems requires a specific operationalization. The data analyzed so far suggests that information asymmetry may provide this specificity. Information asymmetry refers to a potential mismatch between the locus of decision-making and information source. Because integration projects tend to be large, complex and involve multiple stakeholders, such information asymmetry can manifest itself in a number of ways. Consider, for example, the risks identified by the focus group dominated by management (see tables 1 and 2). Information needed to track these risks is likely to be available largely the *other* stakeholders. Due to the distributed nature of these projects, these stakeholders (users and developers) will possess more immediate information about different parts of the project. Advance warnings voiced in different parts of the project, therefore, can contribute significantly to a more effective and early assessment of enterprise integration project risks. As we proceed to the later phases of this research project, we expect to build on this dichotomy to assess of how project participants perceive, track and monitor enterprise integration project risks.

6. References

- [1] S. Alter, and M. Ginzberg, "Managing Uncertainty in MIS Implementation", *Sloan Management Review*, 1978. 20(1): p. 23-31.
- [2] S. Alter, and S. Sherer, "A general, but readily adaptable model of information system risk", *Communications of the AIS*, 2004. 14: p. 1-28.
- [3] H. S. Barki, H., S. Rivard, and J. Talbot, "Toward an Assessment of Software Development Risk", *Journal of Management Information Systems*, 10(2): p. 203-225.
- [4] B. W. Boehm, "A Spiral Model of Software Development and Enhancement", *IEEE Computer*, 1988. 21(5): p. 61-72.
- [5] B. W. Boehm, "Software Risk Management: Principles and Practices", *IEEE Software*, 1991. 8(1): p.32-41.
- [6] C. Brown, and I. Vessey, "Managing the Next Wave of Enterprise Systems: Leveraging Lessons from ERP" *MIS Quarterly Executive*, 2003. 2(1).
- [7] R. Burns, and A. Dennis, "Selecting an Appropriate Application Development Methodology", *The DATABASE for Advances in Information Systems*, 1985. 17(1): p. 19-23.
- [8] J. Carlo, K. Lyytinen, and R. Boland. "Systemic risk, IT artifacts and high reliability organizations: a case of constructing a radical architecture" SPROUTS Working papers at Case Western Reserve University, 2004, 4(2).
- [9] R. N. Charette., *Software Engineering Risk Analysis and Management*, 1989, New York: McGraw-Hill.
- [10] R. N. Charette, "Why Software Fails", *IEEE Spectrum*, 2005.
- [11] S. Collett, "Hershey earnings drop as new warehouse, order systems falter" *Computerworld*, 1999.
- [12] G. B. Davis, "Strategies for Information Requirements Determination", *IBM Systems Journal* 1982.21(1): p. 4-30.
- [13] S. E. Donaldson, and S.G. Siegel, *Successful Software Development*, 2001, Upper Saddle River, NJ.: Prentice Hall.
- [14] M. Earl, *Information Management Strategy*, 1987, Englewood-Cliffs, NJ.: Prentice-Hall.
- [15] K. Ewusi-Mesah, *Software development failures – Anatomy of abandoned projects*. 2003, Cambridge, MA. : MIT Press.
- [16] R. Fairley, "Risk Management for Software Projects", *IEEE Software*, 1994. 11(3): p. 57-67.
- [17] B. Gold-Bernstein, and W. A. Ruh, *Enterprise Integration: The Essential Guide to Integration Solutions*, 2004: Addison Wesley Professional.
- [18] J. Iverson, L. Mathiassen, and P. Axel-Nielsen, *Managing Risks in Software Process Improvement*. *MIS Quarterly*, 2005.
- [19] C. Jones, *Assessment and Control of Software Risks*, 1994, Upper Saddle River, NJ.: Yourdon Press Prentice Hall.
- [20] P. G. W. Keen, and S. Scott-Morton, *Decision Support Systems: An Organizational Perspective*. 1978, Reading, MA: Addison-Wesley.
- [21] M. Keil, A. Tiwana, and A. Bush, "Reconciling user and project manager perceptions of IT project risk: a delphi study", *Information Systems Journal*, 2002. 12: p. 103-119.
- [22] M. Keil et al., "A Framework for Identifying Software Project Risks", *Comm. ACM*, 1998. 41(11): p. 76-83.
- [23] T. H. Kwon, and R. Zmud, "Unifying the Fragmented Models of Information Systems Implementation", in *Critical Issues in Information Systems Research*, R. Boland, Editor. 1987, Wiley: Chichester.
- [24] J. S. Lee, and S. Hong, "Enterprise integration with ERP and EAP", *Comm. ACM* 2003. 46(2): p. 54-60.
- [25] H. Lucas, *Implementation - The Key to Successful Information Systems*, 1981, New York: Wiley.
- [26] K. Lyytinen, and R. Hirschheim, "Information Systems Failure - A Survey and Classification of the Empirical Literature", in *Oxford Surveys in Information Technology*. 1987, Oxford University Press. p. 257-309.
- [27] K. Lyytinen, K., L. Mathiassen, and J. Ropponen, "Attention Shaping and Software Risk - A Categorical Analysis of Four Classical Risk Management Approaches", *Information System Research*, 1998. 9(3): p. 233-255.
- [28] L. Mathiassen, J. Pries-Heje, and O. Ngwenyama, eds. *Improving Software Organizations: From Principles to Practice*. 2002, Addison-Wesley: New Jersey.
- [29] L. Mathiassen, *Systems Integration at Georgia Pacific: Preliminary Results*. 2006, Georgia State University, p. 8.
- [30] R. Montealegre, et al. *BAE Automated System (A): Denver international airport baggagehandling system*. Case study no. 9-396-311. 1996, Harvard Business School Press.
- [31] D. L. Morgan, *Focus Groups as Qualitative Research*, 1988, Beverly Hills, CA: Sage Publications.
- [32] T. Moynihan, "An Inventory of Personal Constructs for Information Systems Project Risk Researchers", *Journal of Information Technology*, 1996. 11: p. 359-371.
- [33] M. Ould, *Managing Software Quality and Business Risk*. 1999, Chichester: Wiley.
- [34] D. Robey and M. Boudreau, "Accounting for the Contradictory Organizational Consequences of Information Technology: Theoretical Directions and Methodological Implications" *Info. Sys. Research*, 1999. 10(2): p. 167-185.
- [35] J. Ropponen, and K. Lyytinen, "Components of Software Development Risk: How to Address Them? A Project Manager Survey" *IEEE Transactions on Software Engineering*, 2000. 26(2): p. 98-112
- [36] J. Scott, and I. Vessey, "Managing risks in enterprise systems implementations", *Comm. ACM*, 2002, 45(4), 74-81.
- [37] K. Siau, "Enterprise Resource Planning (ERP) Implementation Methodologies – Editorial Preface" *Journal of Database Management*, 2004. 15(1).
- [38] M. Sumner, "Risk factors in enterprise wide information management systems projects", *SIGCPR* 2000. Evanston, IL.
- [39] C. Vogt, "Intractable ERP: A Comprehensive Analysis of Failed Enterprise-Resource-Planning Projects", *Software Engineering Notes*, 2002. 27(2): p. 62-68.
- [40] J. B. Wysocki, "Pulling the plug: some firms, let down by costly computers, opt to de-engineer" *The Wall Street Journal*. 1998. p. 1-2.