IT Portfolio Management: An Enterprise Risk Management-Based Perspective

Prasanna Karhade
University of Illinois, Urbana-Champaign

Follow this and additional works at: http://aisel.aisnet.org/amcis2007

Recommended Citation
http://aisel.aisnet.org/amcis2007/405

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2007 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
**IT PORTFOLIO MANAGEMENT: AN ENTERPRISE RISK MANAGEMENT BASED PERSPECTIVE**

**Prasanna Karhade** (karhade@uiuc.edu)
University of Illinois Urbana-Champaign
1206 South Sixth Street, Champaign, Illinois, 61820

**Keywords:** IT Portfolio Management, Enterprise Risk Management, Risk Appetite

**Introduction**

This abstract describes a part of a much larger ongoing, Enterprise IT Strategy Analysis (EISA) (Shaw et. al 2007) project. I am part of a research team that is developing the EISA methodology which involves integrating at least four key components: (1) developing an IT governance framework (Weill and Ross 2004), (2) developing detailed strategy maps (Kaplan and Norton 2004) (3) developing elaborate aggregate project maps (Christensen 1997) and finally (4) IT portfolio management (Maizlish and Handler 2005). This abstract will focus on the IT portfolio management component with an ERM based perspective.

“All management is risk management” is a quote that is often attributed to the famous Canadian risk management pioneer, Douglas Barlow (Shaw 2005). Risk management seems to be at the forefront nowadays in the IT context, as modern CIO offices of large IT-enabled enterprises are expected to justify their enormous investments in IT. Most IT investments are guided not only by the corporate strategy, but also by the risk appetite of the enterprise. The ERM — Integrated Framework published by the COSO of the Treadway Commission, suggests that the risk appetite and the IT investments on an enterprise, should be aligned with the corporate strategy (COSO 2004). In spite of the frequent usage of the risk appetite term, measuring and quantifying this important, but latent, construct seems to be a continuing challenge for IT researchers.

**A Conceptual IT-Risk Framework**

In our EISA project (Shaw et. al 2007), we develop a layered framework to conceptualize IT risk incorporating different types of risk factors relevant to the operation of the modern CIO office.

1. **Technology-related risks:** Security technology and networking equipments and the manner in which these components are integrated together into network configurations are continuously evolving. Thus firms are expected to make continual investments in technology solutions to minimize their exposure to vulnerabilities.
2. **IT vendor- or partner-related relationship risks:** In today’s world of the global software delivery models, firms are growing increasingly dependent on several other firms; including IT service providers, IT consultants, IT vendors and IT auditors. This unavoidable dependence on several IT partners can be arguably viewed as a risk factor.
3. **IT enabled-process and data related risks:** Enterprises today are redesigning their critical business processes around IT applications which enable them to utilize information more efficiently. Key business processes are also likely to span boundaries of multiple enterprises. Thus the fact that confidential data cannot be often constrained anymore within the boundaries of one organization, is emerging as a source of IT enabled process risks.
4. **Compliance related IT governance risks:** Enterprises are now operating in an exceedingly complicated regulatory environment. Enterprises are now expected to invest significant resources to comply with possibly several different regulatory frameworks. These investments can sometimes be industry specific (for e.g. HIPAA compliance for enterprises in the IT enabled health care industry) and thus for enterprises operating in certain industries compliance to regulatory demands and pressures is not an option.
IT Portfolio Management: An ERM-based perspective

Managing IT investments is arguably a big component of ERM. The link between IT portfolio management and ERM is a strong one as ERM advocates IT executives to adopt a holistic, portfolio view of IT risk (THEIIA 2004). A well developed IT portfolio management program is also likely to nurture a strong IT governance regime and can maximize the value of IT investments while minimizing IT related risks (Datz 2003). IT portfolio management (very few papers for e.g. Weill and Vitale 1999), especially the IT portfolio composition process, is relatively understudied. The objective of this research program is study the impact of various sources of uncertainty and risk — described in Table 1, derived partly from our IT risk framework and partly from the ERM Integrated Framework published by the COSO of the Treadway Commission — on the IT portfolio composition decisions.

Model Development

In this research program, we study the IT investment decision-making problem with an emphasis on enterprise risk management by analyzing the entire portfolio of IT investments for a given corporation. These decisions are particularly challenging given evolving IT infrastructure requirements, changing regulatory environments firms operate in and various types of IT-related risks organizations are expected to manage. Though extant literature provides some guidelines for making such strategic IT investments (for e.g. Clemons and Weber 1990), a rigorous investigation of this question can make significant contributions to the IS literature. In particular, a portfolio perspective includes all compliance-related IT investments, IT investments intended for the short-term time horizon and IT investments meant for the long-term time horizon for a given corporation.

In one study, we have developed an enterprise IT-risk management framework and developed scoring models to quantify risk associated with individual IT project investments. These risk factors we use in our research model, are also in agreement to the risk factors suggested by the COSO framework. In another study, using scoring models, we quantify constructs such as business criticality and technological maturity and study their impact on the IT investment decision as illustrated in Figure 1. Thus, we intend to combine multi-dimensional scaling and multiple regression techniques to explain the IT investment decision making problem.

Multi-dimensional scaling can help us represent the risk appetite of organizations as a two-dimensional space on an aggregate project map (Christensen 2000) using business criticality and technological maturity as two dimensions. Further model refinements will include (1) sensitivity analysis and robustness checks of the scoring models (i.e. we will develop alternative scoring models with differing weights assigned to individual components to quantify our main constructs) and (2) analysis of curvilinear relationships between our key independent variables and IT investment decisions (i.e. we will relax the linearity assumption).
Research Method

We adopt a mixed-method research design (Creswell 2003) to study our research problem. Our research methodology (which includes multi-dimensional scaling using aggregate project planning, development of robust scoring models for risk assessment, multiple regression techniques, use of qualitative data, multi-criteria decision making) has been refined over the past six months based on intense collaboration with key corporate industry partners in three industries. All the enterprises that we have worked with so far (three large multi-business multi-national Fortune 500 corporations) have collaborated with us intensely.

Exchange of information between the research team and our corporate industry partners has occurred via several modes including: face-to-face meetings, unobtrusive observation sessions (i.e. during IT investment and planning related corporate meetings), semi-structured interviews with key decision makers, empirical analysis (multidimensional scaling combined with multiple regression) of IT project level data, and follow up telephone conference calls. No method of data collection is perfect in isolation: but when several different modes of data collection are combined, data validation via triangulation can occur.

For our empirical study, we use an individual IT project-based investment as a unit of analysis and IT investment decisions are also made at this project level (i.e. reject project, select project with full funding, select project will partial funding, etc). All this confidential data collected from our collaborating partners is kept strictly confidential. Only the research team has access to this data. All the individuals and corporations participating in our research program choose to remain anonymous.

Expected contributions from our work

Based on results generated from our study, we hope to make significant theoretical contributions. We intend to develop better theoretical understanding of the various risk factors, the interrelationships between these risk factors and how they impact IT portfolio management decisions. We intend to open up the “black box” of the risk appetite of an enterprise and attempt to tease out various technological, organizational and financial dimensions of this construct. We believe results from our study have important managerial implications as well. Studying the IT portfolio management process, with an ERM based perspective, is likely to provide a theoretically grounded, systematic framework which IT executives in CIO offices of large multi-national corporations can use to make well informed IT investment decisions.

Short bibliography of the literature that is most relevant to my work: