Risk –Informed Decision Making in Information System Implementation Projects: Using Qualitative Assessment and Evaluation of Stakeholders' Perceptions of Risk

Monica Schurr
University at Albany
mlmeissner@albany.edu

Manuel De Tuya
University at Albany
mdetuya@albany.edu

Kathryn Noll
Rensselaer Polytechnic Institute
tknoll12@gmail.com

Abstract

The successful implementation of a new software system at any organization requires identification and management of risks as well as insight into the decision-making process throughout the information system lifecycle. Risk assessment of software systems aids in planning, implementation and adoption stages and helps identify potential problems before they occur. This study utilized a qualitative case study method and an interview design for data collection to gather, organize and make sense of key stakeholders' perceptions of risk for decision making in the implementation of a new department-wide computerized system. Top stakeholder risks identified include executive sponsorship support; adoption of the new technologies and processes; and interoperability. The results of the analysis of perceptions of risks allowed the organization and the team responsible for the implementation of the new system to make decisions about mitigating strategies aligned with stakeholders' expectations; forecast potential issues within the implementation timeline based on activities associated with identified risks; and make implementation and process decisions based upon the risk assessment. This study extends the research on IT risk management and decision making by demonstrating the utility and efficacy of a qualitative case study method for eliciting the information needed from stakeholders in order to make decisions regarding system implementation, specifically in an organization that lacks the appropriate risk management maturity level to conduct an exhaustive quantitative analysis of risks associated with the project.

1. Introduction

   This paper describes how a qualitative approach for assessing and evaluating risks in order to inform decision making and risk response benefited a manufacturing organization during and after the implementation of a new department-wide software system. The purpose of the system was to move the organization out of a paper-based manufacturing process and into managing their production process via automated workflows able to control the execution of the manufacturing steps. The organization implementing the system could be characterized as highly concentrated on achieving excellence in their core competencies. Such core competencies, as identified by company executives, fell within the quality assurance and manufacturing areas, with the latter being the actual owner of the system, making the project a department-wide implementation. Nevertheless, the scope of the system required the establishment of a cross-functional implementation team to ensure that cross-departmental processes were considered when configuring the software solution.

   The risk assessment for this study identified risks associated with the new information system, hereinafter referred to as "the system". Risks associated with the system were based on perceptions from areas of business such as Manufacturing, Information Technology (IT), Quality Assurance (QA), Supply Chain, Process Controls, and Management. Traditionally, risk assessments for software implementation projects are performed utilizing a variety of quantitative methods. In the case of the organization being studied, there was a lack of expertise in performing such assessments, in particular for software projects. Using a qualitative method allowed the implementation team access to key organizational representatives of the areas being affected by the system.

   This paper is organized into six sections: section one includes an introduction to the paper in general and this information system implementation project specifically; section two provides a brief literature review; section three describes the methodology;

HICSS

section four presents results; section five analyzes and discusses the interviews and identified risks, and details the risk-informed decision making process that resulted from this work; section six presents limitations; and section seven presents contributions and concluding remarks.

1.1 Description of the Information System Implementation Project

The main goal of the project was to improve productivity and reduce cycle-time in the total time to produce a manufacturing order. Automating the process of controlling manufacturing records would optimize production activities within the organization and most likely bring additional synergies when interacting with external manufacturers. The potential benefits identified during the development of the business cases were, among others, increased productivity, savings in labor costs, enhanced management capabilities, shorter reaction time to changing market conditions and higher availability of manufacturing information throughout the organization.

The proposed approach was to find a best of breed solution that could be integrated into the organization's current technology landscape and long term business and IT strategy. A transformative initiative like this required the establishment of a governance body that included members of the leadership team acting as executive sponsors as well as active members of a steering committee. A project manager from the IT department was in charge of the formal management of the project across the areas of the organization needed in the definition and execution of the project deliverables.

As part of the management of the project, a comprehensive project timeline was produced, which listed a 17-month implementation strategy that included the definition of user and functional requirements, definition of interfaces with other existing applications, unit, system and integration testing phases and a final user acceptance testing phase followed by a month-long deployment into the production environment. The effort was divided into phases as per project management best practices:

- a planning phase where high-level requirements were gathered, vendors were screened and selected and budgets were submitted for approval
- an implementation phase to design and configure the system
- a testing and deployment phase

The interviews for this paper were conducted between the end of the planning phase and the beginning of the implementation phase.

2. Literature Review

2.1. Risk Management for IT Projects

Risks are classified as events that have adverse outcomes. Risk management is a process involving assessment, response and mitigation that can help prevent risk from occurring, as well as minimize damage and contain the cost of recovering from risk, if risk does occur [1]. While risk can never be entirely eliminated from a system, performing risk assessment aids in identifying current or potential risks associated with the implementation and operation of a computerized system in a given organization [2]. Additionally, it can provide strategies to manage identified risks at a level that is acceptable for the organization [3]. Risks are assessed by examining magnitude and likelihood [1, 3, 4], and risk response involves the organization creating and implementing both preventative and corrective controls to ensure risk is minimized [5]. Additionally, risk mitigation acts to introduce controls that reduce potential risks within a system, to address risks and generate solutions to reduce and resolve threats [6].

Risk management within IT systems is vital to ensure that systems operate within specific performance and computational accuracy thresholds previously agreed upon in the form of user requirements and made official via Service Level Agreements (SLAs) [2, 3]. Generally speaking, managing risks in a software implementation project is a three phase process. Each of these phases may present different types of risks and, accordingly, different methods for managing them [7] .

The objective of a risk analysis and identification process is to provide information to facilitate the decision making process related to the implementation of risk management strategies whether it is acceptance, elimination or reduction [8]. Traditionally, risk assessments for software implementation projects rely heavily on a variety of quantitative methods [9-11] that concentrate on the risk analysis and mitigation efforts to project-specific deliverables or processes, which lead to a project-specific decision-making modeling [12]. Nevertheless, software implementation projects produce business-specific (operational) risks that should be quantified and, if needed, managed [9, 13]. To that end, research has demonstrated that involving

business subject matter experts (SMEs) positively impacts the performance of the implementation team and creates a sense of ownership for the SMEs when they perceive the system as their own creation [14]. Appropriately addressing user (SMEs) perceptions of risk have been linked to increased levels of alignment across the business as well as higher levels of organizational awareness [14].

The field of risk assessment and decision making is multifaceted and the processes multidisciplinary, which must be taken into account when considering a scientific platform and/or framework for risk [15]. Many theories explaining risk and decision making form the foundation of quantitative studies for risk analysis and management, including decision theory, the behavioral view of risk, and the real options view of risk [16-18]. While many consider quantitative risk assessment (QRA) the method for estimating and quantifying risk, one must also consider that "societal risk decision making" – which stems from identifying such risks – requires consideration of stakeholders' understandings as well as contextual factors [15]. A qualitative risk assessment targets the elicitation of such important information (i.e. the answers to "what" and "how" questions) and thus provides pragmatic grounds for an exploratory method, which could also lay the groundwork for theory development [19].

2.2. Assessing and Evaluating Risk

Understandings from the field of education with regards to assessment and evaluation can provide a theoretical framework for the development of a qualitative interview protocol, the collection of data on specific risk indicators (assessment) as well as the use of the information gathered from these qualitative interviews to inform decision making on risk management, mitigation, and reduction (evaluation).

One approach in education is to separate the concept of assessment from testing and grading, and understand it as the extent to which one has attained a learning goal; and evaluation can be thought of as applying that assessment information to inform and make decisions [20-22]. For purposes of clarity and precision when measuring attainment, broad learning goals can be written at very specific levels. Specifying (learning) indicators at a fine-grained level as opposed to a coarse-grained level [23, 24] allows for collection of useful information and thus clear and specific measurement of attainment (assessment) as well as actionable evaluation (using the information to inform decisions) and eliminates the potential for confusion that is wrought with

vague, broad, and general statements/indicators [21, 25-27].

In applying this educational assessment and evaluation perspective to the assessment of risk in an IT project, the *indicator of the presence of learning* (i.e. learning goal) can instead be framed in terms of an *indicator of presence of risk (*or, as the case may be, the perceived presence of risk). Furthermore, the concept of coarse-grained and fine-grained information can be applied in terms of broad indicators of risk (e.g. issues with document maintenance) that can be broken down into more specific indicators (e.g. issues with record storage, ease of access, maintaining paper records and need for backups, among others). As in the field of education, collecting this information at such a fine-grained level can inform decisions (what we will call or consider a form of risk evaluation) as much as the actual actions. An example of this is users driving organizational change management, as discussed in the next section.

2.3. Users Driving Organizational Change Management

A determining success factor for the implementation of computerized systems is the level of readiness achieved by the organization prior to deploying the new technology [28, 29]. Such a state of readiness is achieved by the appropriate planning and execution of an organizational change management process [30], which consists of making the organization aware of the change, educating users and secondary stakeholders on the consequences of the change and how to deal with it and creating the corresponding mechanisms so that the new status is adopted as seamlessly as possible [28, 30].

A specific approach for facilitating organizational change consists of involving non-supervisor members of the organization in a semi-crowdsourcing mode of problem solving, also known as participative leadership [31]. Research has positioned participative leadership not only as a generator of trust, but as a driver for enhanced organizational performance [31] and it is also positively influenced by higher degrees of information sharing from supervisors [32]. This approach provides subject matter experts, acting as subordinates of the project leadership team, with intrinsic motivation for finding innovative and effective solutions for specific organizational needs [30, 33].

The inclusion of users (Subject Matter Experts or Stakeholders) in the risk management process should provide a better understanding of perceived risks within the organization [15]. Such risks and their

corresponding mitigation could either hinder or promote the organizational change management process required for the successful implementation and eventual maintenance of a transformative computerized system [11,15]. Applying an assessment and evaluation approach in this context helps to frame the change management process in terms of specific intended outcomes for said processes. Employing assessment at a fine-grained level allows identification of specific risks; employing evaluation allows us to use the information that results from the assessment to make decisions in terms of implementation and maintenance. One can then gather information as to whether the intended outcomes have occurred by using evaluation techniques at the *program* level (see, for example, [34] for a discussion of standards for program evaluation).

3. A Qualitative Approach

3.1 Case Study Research Method

Case studies facilitate the gathering of information necessary for making decisions, as well as focusing on the factors that influenced decisions within each case and then comparing such factors in order to test existing theoretical constructs and relationships [35]. Traditionally, for software implementation projects, risk management is performed by analyzing indicators related to the development or implementation process – requirements complexity, software size, computational complexity and interfacing level, among others. By using an interview design, indicators of risk (via perceptions) can be gathered from a broad range of stakeholders, both technical and non-technical, to gain a better understanding of concerns regarding the effects of the new software on existing processes and computerized systems. More specifically, through semi-structured interviews [36], the level of flexibility facilitates descriptive responses that allow the researcher to develop detailed descriptions, integrate multiple perspectives, develop holistic descriptions and frame hypotheses for quantitative research [37]. Furthermore, qualitative interview techniques lend themselves to: the ability to generate reliable and valid data and reduce bias, such as via consensual qualitative research methods [38]; inductive and deductive methods of analysis [39]; quantification for further analysis [40], as well as laying the groundwork for theory development [19]. The qualitative approach for this study was chosen based

on pragmatic grounds as an opportunity to involve future end users of the system in the identification of risks while gathering their perceptions of the project at large. In addition, the lack of in-house knowledge on performing quantitative risk assessment and the need to keep the timeline unchanged made the method ideal for this particular project.

Participant selection. Interviewees were selected based on level of involvement with the implementation of the system into the company. The total group (N = 27) was selected from manufacturing (N = 11), supply chain (N = 1), IT (N = 5), quality assurance (QA) (N = 4), process sciences (N = 2), and management (N = 4), to encompass a wide range of perceptions associated with implementation of the system.

Data collection approach. This case study research utilized an interview design for accessing and collecting data. Interviews lasted 30 minutes, during which time interviewees' perceptions of risk associated with implementation of the system were recorded.

The interviews were conducted in a semi-structured manner, with a general set of questions prepared, but improvisation was used to obtain more specific information based on the subjects' knowledge and experience with the system.

For each department, a different set of exploratory "what" and "how" questions were used in order to elicit the thinking and opinions of each respective group [19]. Sample questions included: "What are the main risks you feel the system could generate for manufacturing that would interfere with the benefits of the system?" (Manufacturing); "How will implementation of the new system affect the functionality of current systems?" (IT); "What could be the risks if data integrity is compromised?" (Supply chain); "How could implementing the system affect compliance?" (Quality Assurance); "What are the potential impacts or risks if the system is not accurate?" (Process sciences).

Coding and data processing methods. Interview transcripts were reviewed after each interview to ensure that the proper meaning of the interviewees' responses were recorded. These interview transcripts were broken into smaller units, based on categories created to reflect the main ideas of the responses gathered. For each interview question asked, the number of people surveyed was recorded; this was followed by responses to the question in unitized, coded form, listing category and subcategory, as well as the participant's identification number and

department. Any repetitions of responses or units for each person was counted, but not listed as a separate response, to allow for more comprehensive data analysis and to avoid skewing the data by the inclusion of redundant responses. Sorting and coding was done by hand to ensure the proper meaning behind responses was captured.

Categories and subcategories were generated after reviewing the data, to ensure main themes were accurately captured within the codes; to represent different types of risk expressed by employees; and to allow for more precise and specific identification of risk indicators (assessment) as well as inform the resulting decisions for action (evaluation).

Categories were broken into types of risk, as well as benefits the system can offer and potential controls suggested by subjects. Subcategories broke these categories down into more fine-grained, specific topics, to allow for the analysis to address more narrow ideas, which aided in identifying risks by eliminating the confusion inherent in broadness and generality. Responses were broken into units that were then coded based on this category scheme. Coded responses were transferred to Microsoft Excel spreadsheets and included participants' identification number, department, category, and subcategory of code for each question response.

Using Excel, responses were analyzed based on frequency of response. The coding established for categories and subcategories was used to identify similar perceptions and establish the frequency of similar responses of risk. Data were analyzed for frequency of category and subcategory, as well as to identify if there were common responses within departments. From this analysis, risks were identified, based on the most common risk perceptions, as well as their potential impact to the operations, finances or compliance commitments of the company[1].

4. Results

4.1. Identifying Common Perceptions of Risks – Themes

Overall common perceptions of risks by frequency of theme. Based on the thematic categorization scheme used, we found that the most common perceptions of risk were associated with document maintenance, adoption of the system, support for the system from the company, and

connectivity of the new system with existing systems. The results of the most commonly occurring main categories of risk are found in **Figure 1**.
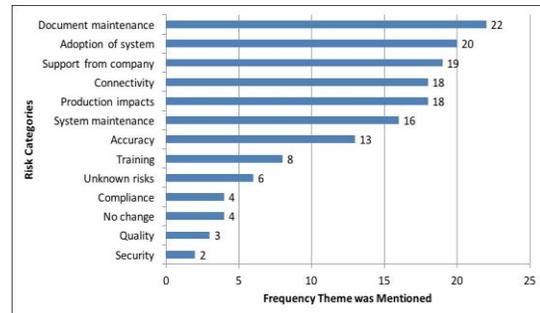
Figure 1: Results of overall perceptions of risk, based on 27 employees interviewed.

Subcategories for each category presented in **Figure 1** were also assessed for frequency of response. The most common risk perceived from the study was the risk associated with record set-up and review quality, with 21 out of 27 responses. Risks associated with delays to processing time (i.e. the performance of the system was suboptimal) was the second highest concern, with 16 out of 27 responses.

The most common perceptions of risk, based on 27 subjects interviewed, are found in **Table 1: Top eight most common perceptions of risks from 27 interviewed**. An example of subcategories of risks perceived is displayed in **Figure 2**. Quotations from subjects support these perceptions of risks, e.g.:

- Regarding risks associated with delays to processing time: *"Sites can grind to a halt if [the system] is not set up correctly."*
- Regarding risks to adaptation of business practices: *"The issue is with [the company] adjusting to the system, not the system changing to meet what the company does."*
- Regarding risks to support: *"For [the system] to be successful, we need the right people, the right resources, and support."*
- Regarding risks associated with data accuracy and interoperability *"If we are not disciplined in data entry in other systems as we are with [the new system], it could take down [the new system], in terms of reporting incorrect data"*

Table 1: Top eight most common perceptions of risks from 27 interviewed

---

[1] For the complete set of interview questions and categorizations for coded responses, please contact the authors at mlmeissner@albany.edu.

Risk Perception	Number of Responses
Record Set-up/review quality	21
Delays to Processing Time	16
Adoption of the system	13
System Unavailability	12
Adaptation of business practices	11
Connectivity to other systems	11
Lack of experience on-site	10
Need for backups of system	9

Figure 2: Results of risks perceived

Common perceptions of risk by department. Responses were also analyzed to see if any patterns of risk perceptions existed within departments. These results are shown in **Figure 3**. IT was most concerned about support from the company for the project. Manufacturing was most concerned about risks regarding adoption of the system and risks to document maintenance. Management was focused on the top four categories of support, connectivity, adoption of the system, and document maintenance. QA was most concerned about document maintenance risks and potential impacts to production.
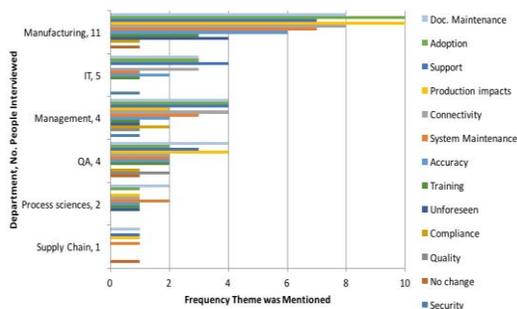

Figure 3: Results of main categories of risk perception by department.

Common perceptions of benefits. Participants (N = 24) were also interviewed regarding the perceived *benefits* that the new system would offer the company. The responses indicate that reduction in production time and reduction in work were the most common perceptions. The results are shown in **Figure 4**. A breakdown of benefits by department is in **Figure 5.** Employees interviewed in manufacturing responded most frequently that the system would increase accuracy. In IT, the most common perception of benefits was a reduction in production time and work. In QA, the common perception was that the system would allow for an increase in compliance.
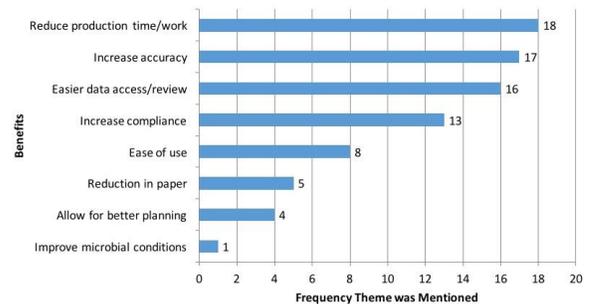

Figure 4: Results for perceptions of benefits for the new system.
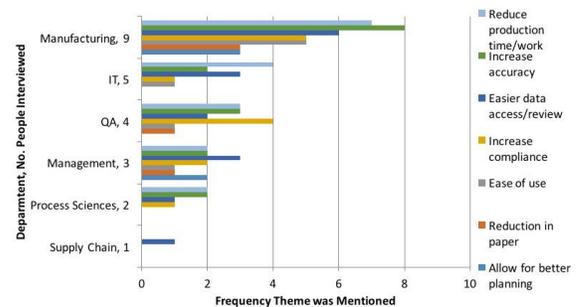

Figure 5: Results for perceptions of benefits, by department.

5. Discussion

From this study, the main risks to implementing the new system revolved around document maintenance, adoption of the system, support from the company in the form of executive sponsorship and connectivity of the new system with other existing software systems, i.e. interoperability of the new software. These perceptions of risk stemmed from the level of involvement of the interviewees with the implementation of the software system, as well as experience and knowledge of the software

package. The results of this study suggest that the most common perceptions of risk also pose as the most impactful in the minds of the interviewees. Nevertheless, adoption, executive sponsorship and interoperability with extant applications have previously been negatively associated with the successful implementation and subsequent maintenance of large software projects [29].

From the analysis of frequency of perceptions of risk by department, certain patterns arose regarding perceptions of risk. For manufacturing, the main concerns of risks focused on *operational* (manufacturing of the company's main products) impacts and adoption of the system. IT had the largest frequency of responses of risk perceptions regarding *support* for the system, as IT's function would be to ensure that the operation of the system complies with the service level agreements in place between the operational areas of the business and IT. Results related with the Quality Assurance (QA) area were risks to *document maintenance*, which is key to the organization since the vast majority of their standard operating procedures, work instructions and many other compliance-related artifacts are paper based and would need to be maintained even during a period of time where system and paper would run in parallel. The importance of the roles of Manufacturing, QA and IT in implementing and sustaining the new system reinforce the idea that if the risks identified for each area are not properly addressed, the overall performance of the organization might be jeopardized [2, 5].

From the risks identified, mitigation strategies should be established to aid in the transition to the new software system. Following the assessment and evaluation framework proposed earlier, one can determine the extent to which such strategies are effective at addressing risks[2].

5.1 Discussion of the Risk-Informed Decision Making Process

This discussion is framed by the following: each of the broad areas of risk and then more specific perceived risks; proposed strategies;[3] decisions and actual changes that were implemented; and results of the changes.

5.1.1 Document maintenance. *Perceived risk* – The information being entered in the system, manually or

automatically, is incorrect and will therefore generate errors in the manufacturing process.
Proposed strategy - Testing record set-up within the system and having a process to validate records in place before having the system go live.
Actual Change - This proposal led to the design of a comprehensive user acceptance testing strategy that was able to tie back the initial user requirements to the functional design and to the results of the testing scripts of the user acceptance phase.
Results - By the time this study was concluded, the implementation team was ready to execute the set of user acceptance scripts described in the testing plan.

5.1.2 Data Retrieval and System Availability.
Perceived risk – In case of a system failure, the recovery process compromises the integrity and completeness of the data.
Proposed strategy - Establishing redundant systems to act as backups for data and records if the original system is unavailable.
Actual change - In order to mitigate this risk, the Information Technology infrastructure team collaborated with the software vendor to design a resilient architecture that not only ensured the integrity of the data, but also enabled high availability capabilities by implementing failover mechanisms from the production servers to back up servers for the application, database and web servers.
Results - The results of the enablement of the high availability, full recovery architecture for the system gave the organization a sense of reliability on the mechanisms provided by the Information Technology department once all the failover, backup and recovery features were fully tested. The testing involved loading a test instance of the system with a set of controlled test data, making the system unavailable unexpectedly and then recovering the full set of test data.

5.1.3 System Adoption. *Perceived risk* - Increased implementation and operational complexity originated by the customization of the software to fill unnecessary business requirements.
Proposed strategy - Adopt business practices to the system, not changing the system to meet what the company does [as this introduces new risks of losing functionality of the system].
Actual change - A direct mandate from the management team instructed the implementation team to keep customization of the software down to a minimum. This would ensure that system functionality was standard while forcing the impacted business areas to actually change their business processes.

---

[2] Although this has not been done as of the writing of this paper.

[3] These strategies were proposed by a group of stakeholders and were captured as part of the interview process.

Results - The configuration of the system was completed with zero customizations to its core functionalities. One customization was authorized that dealt with interfacing the new system with the inventory management system.

5.1.4 System rollout. *Perceived Risk* - Lack of understanding on how to interact with the new system, which could lead to costly errors in the manufacturing process.

Proposed strategy - Ensuring positive communication is maintained between all stakeholders, stressing the importance of the system and the benefits the system can bring to the company.

Actual change - Executive involvement played a key role in the advertisement of the new system, its capabilities and potential benefits. Senior management leaders were constantly stressing the importance of the new technology being implemented and labeled the implementation project as the highest priority from a technology perspective across the company.

Results - The organization is well aware of the scope and the status of the implementation project as well as the benefits and changes the system will bring to all areas impacted. By having access to this information, people were able to proactively prepare for the transition, resulting in easier execution of the organizational change management phase of the system.

5.1.5 Lack of experience. *Perceived risk* - The organization would not be able to fully realize the benefits of the system because the vast majority of its workforce has never operated a system like this.

Proposed solution - The company could gain expertise onsite by converting experienced consultants and contractors to fulltime employees, also reducing the risk of not having enough support staff onsite.

Actual change - The organization started training the future system experts very early in the implementation phase. In addition to receiving full operational training from the vendor, these resources started configuring testing scenarios in a sandbox instance of the system by transforming actual manufacturing processes into usable configuration.

Results - The newly trained resources were able to become proficient in the configuration of the new system in a relatively short time. This very fact opened the door for establishing an ambitious yet realistic and feasible train-the-trainer approach. By the end of the configuration phase of the system, the manufacturing organization was well positioned to

fill any potential operational need related to the new system.

5.1.6 Connectivity – Interoperability. *Perceived risk* - The organization may face issues integrating the new system into its existing technology landscape, which could result in having inaccurate and/or incomplete data.

Proposed Solution - Reviewing all the systems onsite to ensure data is consistent between systems, to reduce confusion. A plan should be established to ensure all systems are maintained and up-to-date, to reduce risks of incorrect or out-of-date information being shown in the new system. Communication between system owners, with regards to system downtime and updates and coordinating this between systems, needs to be established, in order to better plan for any potential impacts to the new system.

Actual change - The Information Technology department embarked on the implementation of a middleware based on the service-oriented architecture paradigm. This new piece of technology would ensure a more precise and accurate integration between any existing system that needed to provide data and the new manufacturing system.

Results - The implementation of the middleware called for a very detailed list of data points to be exchanged between the manufacturing system and other systems. This approach made for a clear and limited initial scope of interfaces while building a scalable platform for future needs.

The enactment of the actual changes described above came at different stages of the implementation project and in most cases were the result of discussions between senior management and the implementation team backing their argument on the perceived risks and the proposed strategies of the subject matter experts.

6. Limitations

Direct quotations of the subjects' responses could not always be recorded. Data analysis methods have questionable reliability as category generation and coding was performed by one person. Future directions for this study include reducing potential bias of the data analysis by using quality criteria measures, such as an intercoder consistency-matrix [40] or Consensual Qualitative Research methods [38].

7. Conclusions and Contributions

Organizations like the one studied in this paper are often challenged with applying formal, rigorous methodologies to ensure high-quality deliverables and minimal disruptions to their operations when implementing technology projects. The results from this work extend the research on IT risk management and decision making by demonstrating the utility of a qualitative case study method for identifying perceived risks from key stakeholders in order to make decisions regarding system implementation. Such methods allowed for a wide range of perceptions of risk to be gathered from future end users of the system without over-allocating project or operational resources and without having to source in a skillset that was not available within the IT organization. A decision making process was followed for articulating high-level risk mitigation plans based on perceived risks obtained from qualitative interviews.

While the process may differ from traditional quantitative risk management methodologies, our research shows this method to be effective and efficacious by a) delivering a viable alternative for the appropriate identification of risks for resource and time constrained organizations; b) providing solid information for driving the decision making process around risk mitigation strategies; and c) being conducted within a specific timeline bounded by the overall project schedule. Finally, our research confirmed the value of involving key stakeholders and business subject matter experts in the identification and potential mitigation of risks in transformative technology projects by facilitating acceptance and approval of our results and suggestions of risk management strategies when presented to company executives.

Future work may include a deeper analysis on how key stakeholders and subject matter experts contribute to the success of such transformative initiatives and how their actual decision making process enriches such contributions. Adoption of more targeted assessment and evaluation methods-- including a consideration of the techniques and standards associated with program evaluation--may also contribute to the organizational change management process and assist organizations with realizing the intended outcomes of such change.

References

1. Hopkin, P., *Risk Management*. 2013, Kogan Page.
2. Carcary, M., *IT Risk Management: A Capability Maturity Model Perspective.* Electronic Journal of Information Systems Evaluation, 2013. **16**(1): p. 3-13.
3. Javani, B. and P.M.D. Rwelamila, *Risk management in IT projects – a case of the South African public sector.* International Journal of Managing Projects in Business, 2016. **9**(2): p. 389.
4. Rodriguez, A., F. Ortega, and R. Concepcion, *A method for the evaluation of risk in IT projects.* Expert Systems with Applications, 2016. **45**: p. 273-285.
5. Tams, S. and K. Hill, *Information systems project management risk: Does it matter for firm performance?* Journal of Organizational and End User Computing, 2015. **27**(4): p. 43-60.
6. Boehm, B., *Software Project Risk and Opportunity Management.* Software Project Management in a Changing World, 2014: p. 107.
7. Stoneburner, G., A.Y. Goguen, and A. Feringa, *SP 800-30. Risk Management Guide for Information Technology Systems.* 2002, National Institute of Standards \& Technology.
8. Samadi, H., S. Nazari-Shirkouhi, and A. Keramati, *Identifying and Analyzing Risks and Responses for Risk Management in Information Technology Outsourcing Projects Under Fuzzy Environment.* International Journal of Information Technology & Decision Making, 2014. **13**(6): p. 1283-1323.
9. Chae, B. and M.S. Poole, *Mandates and technology acceptance: A tale of two enterprise technologies.* Journal of Strategic Information Systems, 2005. **14**: p. 147-166.
10. Akomode, O.J., B. Lees, and C. Irgens, *Constructing customised models and providing information to support IT outsourcing decisions.* Logistics Information Management, 1998. **11**(2): p. 114-127.
11. Pan, C.g. and Y.w. Chen. *An Optimization Model of CMMI-Based Software Project Risk Response Planning.* 2006. Egypt, World Academy of Science Engineering and Technology.
12. Ben-David, I. and T. Raz, *An Integrated Approach for Risk Response Development in Project Planning.* 2001, Macmillan Press. p. 14.
13. Lyytinen, K. and M. Newman, *A tale of two coalitions - marginalising the users while successfully implementing an enterprise resource planning system.* Information Systems Journal, 2015. **25**(2): p. 71-101.
14. Spears, J.L. and H. Barki, *Special issue user participation in information systems security risk management.* MIS Quarterly, 2010. **34**(3): p. 503-522.
15. Aven, T. and E. Zio, *Foundational Issues in Risk Assessment and Risk Management.* Risk Analysis, 2014(7): p. 1164.
16. Arrow, K.J., *Aspects of the theory of risk-bearing.* Yrjö Jahnsson lectures 1963. 1965: Yrjö Jahnssonin Säätiö.

17. Benaroch, M., *Managing Information Technology Investment Risk: A Real Options Perspective.* Journal of Management Information Systems, 2002. **19**(2): p. 43-84.

18. March, J.G. and Z. Shapira, *Managerial Perspectives on Risk and Risk Taking.* Management Science, 1987. **33**(11): p. 1404-1418.

19. Yin, R.K., *Case study research : design and methods*. Applied social research methods series. 5. 2003: Sage.

20. Johnson, M., *Definitions and models in curriculum theory.* Educational Theory, 1967. **17**(2): p. 127-140.

21. Johnson, M., *Intentionality in Education*. 1977, Albany, NY: Center for Curriculum Research and Services, State University of New York at Albany.

22. Johnson, M., *Curriculum's Missing Data Base.* Curriculum Inquiry, 1985. **15**(4): p. 359-360.

23. Andrade, H. and G.J. Cizek, *Handbook of formative assessment*. 2010: Routledge.

24. Pellegrino, J.W., *Assessment as a positive influence on 21st century teaching and learning: A systems approach to progress.* Psicología Educativa, 2014. **20**(2): p. 65-77.

25. Popham, W.J., *Curriculum matters.* Kaleidoscope: Contemporary and Classic Readings in Education, 2009: p. 113.

26. Sawyer, R.K., *The Cambridge handbook of the learning sciences*. 2005: Cambridge University Press.

27. Tyler, R.W., *Basic principles of curriculum and instruction*. 2013: University of Chicago press.

28. Sofat, K., R. Kiran, and S. Kaushik, *Management of Organizational Change and its Impact on Commitment: A Study of Select Indian IT Companies.* Global Business & Management Research, 2015. **7**(3): p. 69-86.

29. Englund, R.L., A. Bucero, and K.H. Rose, *Project Sponsorship: Achieving Management Commitment for Project Success.* Project Management Journal, 2016. **47**(1): p. e1-e1.

30. Morin, A.J.S., et al., *Longitudinal associations between employees' beliefs about the quality of the change management process, affective commitment to change and psychological empowerment.* Human Relations, 2016. **69**(3): p. 839-867.

31. Miao, Q., A. Newman, and X. Huang, *The impact of participative leadership on job performance and organizational citizenship behavior: distinguishing between the mediating effects of affective and cognitive trust.* International Journal of Human Resource Management, 2014. **25**(20): p. 2796-2810.

32. Lam, C.K., H. Xu, and S.C.H. Chan, *The Threshold Effect of Participative Leadership and the Role of Leader Information Sharing.* Academy of Management Journal, 2015. **58**(3): p. 836-855.

33. Sagnak, M., *Participative Leadership and Change-Oriented Organizational Citizenship: The Mediating Effect of Intrinsic Motivation.* Katılımcı Liderlik ve Değişim Yönelimli Örgütsel Vatandaşlık: İçsel Motivasyonun Aracılık Etkisi., 2016(62): p. 199-212.

34. Yarbrough, D.B., et al., *The Program Evaluation Standards: A Guide for Evaluators and Evaluation Users: A Guide for Evaluators and Evaluation Users*. 2010: Sage Publications.

35. Yin, R.K., *Case study methods*, in *APA handbook of research methods in psychology, Vol 2: Research designs: Quantitative, qualitative, neuropsychological, and biological.*, H. Cooper, et al., Editors. 2012, American Psychological Association: Washington, DC, US. p. 141-155.

36. Myers, M.D. and M. Newman, *The qualitative interview in IS research: Examining the craft.* Inf. Organ., 2007. **17**(1): p. 2-26.

37. Weiss, R.S., *Learning from strangers : the art and method of qualitative interview studies*. 1994: Free Press u.a.

38. Hill, C.E., et al., *Consensual qualitative research: An update.* Journal of counseling psychology, 2005. **52**(2): p. 196.

39. Burnard, P., et al., *Analysing and presenting qualitative data.* British Dental Journal, 2008. **204**(8): p. 429-432 4p.

40. Srnka, K.J. and S.T. Koeszegi, *FROM WORDS TO NUMBERS: HOW TO TRANSFORM QUALITATIVE DATA INTO MEANINGFUL QUANTITATIVE RESULTS.* Schmalenbach Business Review (SBR), 2007. **59**(1): p. 29-57.