Received 26 March 2007
Revised 19 October 2007
Accepted 27 November 2007

Supporting decision making in risk management through an evidence-based information systems project risk checklist

Lihong Zhou, Ana Vasconcelos and Miguel Nunes
Department of Information Studies, University of Sheffield, Sheffield, UK

Abstract

Purpose – This paper aims to present a study of Information Systems project risk management aimed at identifying a risk ontology and checklist that will enable decision making and mitigation strategy planning in information system (IS) development in the public sector. This sector is an ideal research field in risk management practices, due to the visibility that failure of IS/IT projects has acquired as a consequence of the duty of accountability that characterises it.

Design/methodology/approach – The study is based on a qualitative approach anchored on a critical literature review, leading to the development of an analytical framework, followed by a thorough case-study survey.

Findings – A project risk ontology was derived from the analysis of ten case-studies in the UK, USA and New Zealand and was divided into five main categories: pre-project, customer, project management, technological issues, and development methodology. The analysis found that a considerable number of risk factors are incurred before the start of the formal project and pre-determine the future of the project and create predictable risks that can be avoided.

Research limitations/implications – This paper has focused on the pre-implementation and implementation phases of IT/IS projects and further research into IS post-implementation is required.

Originality/value – The proposed ontology is designed to fit in real life systems development cycles and is aimed at supporting risk assessment and control. The findings suggest that risk thinking should start early in the project and not, as many modern design and development methodologies propose, solely as part of the development process itself.

Keywords Information systems, Risk management, Risk analysis

Paper type Research paper

1. Introduction

Risk assessment is a vital process in any effective information system (IS) development. In fact, risks are intrinsic to any project and risk taking is a necessary component of any process of decision making. Poor risk management of IS projects often leads to failure, a situation not uncommon in both the public and corporate community. Failures have been linked to incorrect market positioning, inadequate business and risk strategies, poorly informed decision making based on insufficient information and without due authorisation from senior management (Nunes and Annansingh, 2002). Also, the situation is often intensified by absence of clearly defined risk limits, deliberately misleading reports, inadequate intra-organisational communication concerning risk vulnerability, superficial or unrealistic risk control, poor knowledge of the business environment and lack of timely decision making.

Information Management & Computer Security
Vol. 16 No. 2, 2008
pp. 166-186

0968-5227
DOI 10.1108/09685220810879636

As a result, various interested parties such as shareholders and other corporate entities are deprived of valuable information, which could lead to the formulation of more comprehensive and reliable risk systems, particularly as they relate to information systems.

However, as proposed by Keil *et al.* (1998), "before we can develop meaningful risk management strategies, however, we must identify these risks." Risk is the occurrence of an event that has consequences for, or impacts on, IS projects (Kliem and Ludin, 2000). As stated by Cadle and Yeate (2001), all projects involve risk of some sort. According to these authors, this risk may stem from the nature of the work – for example if there is considerable amount of innovation involved – from the type of resources available, from the contractual relationship which is in place or from the political and social factors which influence the project. Therefore, in order to better understand risk and its consequences, Charette (1989) proposes an useful conceptual overview of risk:

> First, risk concerns future happenings. Today and yesterday are beyond active concern, as we are already reaping what was previously sowed by our past actions. The question is, can we, therefore, by changing our actions today, create an opportunity for a different and hopefully better situation for ourselves tomorrow. This means, second, that risk involves change, such as changes of mind, opinion, actions, or places [. . . Third] risk involves choice, and the uncertainty that choice itself entails. Thus, paradoxically, risk, like death and taxes, is one of the few certainties in life.

This overview of risk is particularly relevant when considered in the context of IS design and development processes. In fact, as discussed by Pressman (1997, p. 141), the future is our concern and the project manager must be prepared to identify risks that may cause the IS project to go off-track. By the admission of Charette (1989), this may in itself be an impossible task. In support of this idea, Drucker (1975) had previously proposed that:

> While it is futile to try and eliminate risk, and questionable to try and minimise it, it is essential that the risks taken are the right risks.

So, if it is not practical to eliminate risks altogether; it must certainly be possible to manage projects in a way that recognises the existence of the risks and prepares, in advance, methods of dealing with them if they occur (Cadle and Yeate, 2001). This entails two major activities risk analysis and risk management. Risk identification, valuation and assessment are therefore the fundamental basis to support the entire risk management process (Nunes and Annansingh, 2002).

This paper aims at proposing a risk identification ontology, in the form of a checklist that aims at supporting risk assessment, decision making concerning risk control and the planning of risk mitigation strategies. This ontology was constructed through an evidence-based approach closely linked to the reality of development and an analysis of failure emerging from real-life case-studies.

2. Research methodology

2.1 Research question

The research presented in this paper was driven by the general aim of helping project managers and practitioners in their risk thinking, assessment and decision making. The literature in the field offers a rich variety of risk management frameworks and model,

such as Drori (1997), Keil *et al.* (1998), Kasser (1998), Sumner (2000) and Bronte-Stewart (2005). Therefore, and after an indicative literature review it was noted that it is in the risk analysis processes that contributions for practitioners are in actual need. Namely, in clear checklists that can be used at the planning phase and as the basis for risk assessment. Checklists are valuable planning and assessment devices when carefully developed, regularly updated, validated and applied. A sound checklist specifies and clarifies the criteria that should be considered when assessing a phenomenon in particular context and supports the evaluator not to forget important criteria (Stufflebeam, 2000). In terms of risk assessment, a checklist enhances the objectivity and credibility of the evaluation process and guides practitioners in planning for the outcomes of the evaluation. As Stufflebeam (2000) puts it, in the quality vernacular, "checklists are useful for both formative and summative evaluations."

Consequently, the following overarching research questions were formulated:

RQ1. What constitutes a good IS project risk identification checklist?

RQ2. How can a risk identification checklist be created?

RQ3. What should be the content of such a checklist?

In responding to these main research questions, the project then aimed at producing an extensive risk identification checklist that could be used by both practitioners and IS risk researchers.

2.2 Research design

In attempting to respond to the above research questions and aims, this research project employed an inductive qualitative research methodology through a combination of critical literature review and a process of case-study survey. Specifically, this research was performed using a desk study approach, exclusively using secondary sources. Desk studies are usually equated to literature reviews. Jackson (1994) defined desk research as "the process of accessing published secondary data." This is an extraordinarily poor and reductionist definition because merely assessing and synthesizing secondary sources does not necessarily add to the current body of knowledge in a particular field (Bhandari *et al.*, 2005). This notion is clearly stressed by Remenyi *et al.* (1998), when arguing that this type of study must be a critical evaluation of the thoughts of other academics, rather then merely accepting secondary sources on face value. However, the traditional critical literature process aims to demonstrate a critical awareness of background studies and takes place early in research projects for construct validity purposes (Gill and Johnson, 1991).

The study reported in this paper, however, aimed at having the desk study as the main method of research and not just as a construct validity vehicle. The strategy here is to adopt an inductive argument in order to explore failure and problems as experimented by different organisations, through the analysis of published and publicly available case-studies. Therefore, this study adopts a desk research approach through critical case-study survey analysis, that is, the study surveys non-theoretical secondary sources, based on applied research. The general approach to the critical analysis is inductive in nature, as it is believed that it is possible to infer general truths from the particular, that is induce theoretical conclusions from specific cases (Walliman, 2001).

An inductive approach starts with a question or "problem statement" (Glesne and Peshkin, 1992) followed by conclusions that are generated from the existing data. Research using this approach is particularly concerned with the context in which such events take place; therefore, the study of a small sample of subjects may be more appropriate than a large number (Easterby-Smith, 2002). Thus, it is hoped that the selection of a meaningful and representative sample of case-studies may provide a good basis for a good critical analysis that may result in generalisable understandings (Bhandari *et al.*, 2005). Furthermore, as stated by Saunders *et al.* (2000), inductive research allows a more flexible approach, as changes, in stance and sample, can be made as the research progresses. Based on these arguments, the methodological framework on Figure 1 was adapted from Bhandari *et al.* (2005). This framework encompasses the following four inductive steps and is based on the framework proposed by Yin (1984):

(1) Performing a critical literature review on IS risk management and risk assessment was carried in order to provide a theoretical background to the study and establishing an initial proposition of main categories of risk in IS development for further exploration and critical analysis.

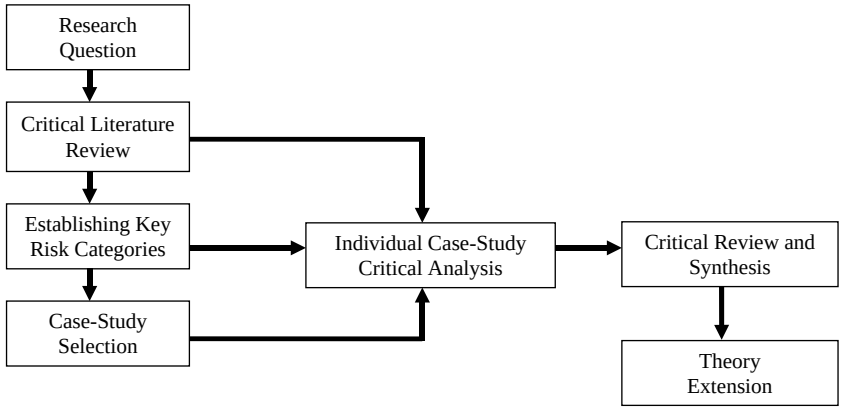
(2) Establishing an appropriate set of case-studies was selected on the basis of its validity, descriptive value and reliability (in this case: ten public sector case-studies following an Anglo-Saxon tradition).

(3) Performing an analysis of individual case-studies by using the key set of categories and theoretical knowledge as guides.

(4) Producing a synthesis of the different case-studies to provide a response to the research question and to establish the risk identification ontology.

2.3 Case-study survey and analysis

Case-study analysis is not a common approach in social sciences used to explore and understand complex and localised human activity systems and social environments. Some of the classic studies in organisational research have been derived from such detailed investigations of organisations (Bryman, 2002). The term "case study" has multiple meanings. It can be used to describe a unit of analysis (for example, a case study



Source: Bhandari *et al.* (2005)

Figure 1.
Framework of a case-study survey inductive approach

of a particular organisation) or to describe a research method. Case study is generally accepted as a qualitative research method (Alavi and Carlson, 1992; Orlikowski and Baroudi, 1991) and according to Saunders *et al.* (2000, p. 94), it is an approach particularly suited to generates answers to the questions "why," "how," and "what":

> A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident (Yin, 1984).

However, the approach adopted in this study is not a traditional case-study approach, but rather the surveying and cross-case critique of the findings of case-study analysis undertaken by others. It uses case-study findings as secondary data because of the contextualised and applied nature of that type of research.

After careful consideration, it was decided that in order to identify risks in IS projects, the natural strategy would be to study and analyse cases of failure of this type of project. Past failure causes and events, can be interpreted as risks in future projects.

Since 1960s, a very large number of information systems have been developed in both private sectors and public organizations. In the most recent decades, the number has increased exponentially. Nevertheless, the high rate of information system failure has become a persistent and continuously topical issue. It could be reasonably be expected that with the accumulated experience of decades of design and development in the IS/IT sector would achieve better rates of success. However, as stated by Lawrence (2003), "IT project management is still very poor compared with other industries, and lessons are not being learnt." In fact, decades of studies on failures of IS development have not substantially decreased the failure rate. These failures have been extensively documented and studied (Clegg *et al.*, 1997; Keil *et al.*, 1998; Whittaker, 1999; Fielding, 2002; Jaques, 2004, Bronte-Stewart, 2005). This persistent failure turns Martin Cobb's paradox (Voyages, 1996), as topical today as it was a decade ago: "we know why projects fail, we know how to prevent their failure, so why do they still fail?"

This failure has had different degrees of visibility. In particular, the failure of IS projects in the public sector has been the "media delight" (Harrin, 2007) for a number of years now, due to the requirements for transparency and accountability in the sector. In no other sector are IS/IT projects perceived to have been so plagued by failure and ongoing problems. This is reflected in the number of such case-studies being currently used in teaching and training situations, and on the growing public concern on this type of project. In the UK, this is clearly illustrated in a recent report put together by the Parliamentary Office of Science and Technology in 2003 entitled "Government IT projects" that aims to improve the success rate of public sector IT projects and highlight common pitfalls. This visibility is due the duty of accountability that forces the sector to disclose any emerging failure and submit to the scrutiny from political and social institutions. This certainly makes IT projects in the sector more vulnerable to criticism and public inspection, but also makes these projects an ideal research instrument in risk management practices. Therefore, the research team behind this study took the deliberate decision to select ten case-studies from an Anglo-Saxon tradition Public Sector, as shown in the Appendix, specifically from the UK, USA and New Zealand. This choice is rooted on the very high levels of transparency, detail, trustworthiness and credibility of the information disclosed about these failures.

This was perceived to be appropriate since in terms of generalisation, there should be no significant difference in risk management between the private and the public sector, as defended by Hood and Rothstein (2000). Nevertheless, although these case-studies are all from the public sector, they represent different areas of application and different national contexts, albeit in an Anglo-Saxon environment. The intention was to, within the same sector; cover a diversity of areas of application and of organisational context.

The additional quality criteria for the selection of case-studies included the following characteristics:

- clear and descriptive;
- focus on failure description and discussion; and
- findings are unbiased and supported by sound research framework.

2.4 Establishing key risk categories from a critical literature review

There is a vast and rich amount of both professional and academic publications addressing IS design and development and their associate risks (Charette, 1989; Keil *et al.*, 1998). The urgent necessity of risk management is recognised to be not only obvious and inevitable, but also complex and difficult to implement. From a distillation of this literature, it emerged that most project management authors focus on procedural aspects of the management process such as estimation, planning, monitoring, team building and change management (Chapman and Ward, 1997; Kliem and Ludin, 2000; Mantel *et al.*, 2001; Pritchard, 2004). Conversely, most software (SW) engineers and computer science authors focus on technical problems of the design and development process that is requirement specification, abstract representation of human activity systems and information environments, programming, testing and installation (Drori, 1997; Jalote, 2002; Taylor, 2003; Tsui, 2004). However, practitioners require a more integrative and holistic approach in order to be able to think about risk in context and take decisions on avoidance and mitigation of these risks (Brown, 2000). Therefore, this study developed such a holistic conceptual model shown in Figure 2, based on the five main dimensions of an IS project: pre-project, customer, project management, technological issues, and design and development methodology.

This holistic conceptual model aimed at establishing a manageable set of key risk categories in order to proceed with the analysis of the case-studies as proposed in the

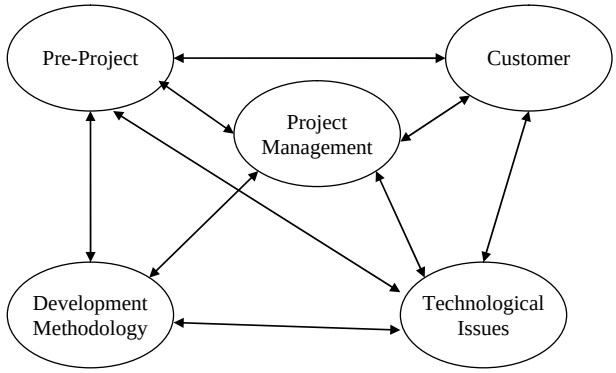


Figure 2.
Holistic conceptual risk model

research framework shown in Figure 1. The conceptual model itself resulted from the critical literature review and a synthesis of a number of existing holistic models. In particular, the conceptual model proposed was strongly influenced by propositions by Hughes and Cotterell (2002) and Cadle and Yeate (2001).

3. Research findings

3.1 Pre-project

Pre-project preparations and contracting are critical to the success of any type of project (Dvir *et al.*, 1998). Before the project kicks-off, both the project team and the customer need to have a good and agreed understanding of the requirement specifications, contractual relationships, project scope and constraints (e.g. budget, technology in use, interfaces with other systems both internal and external, etc.), organisational environment, as well as the business environment. Cadle and Yeate (2001) proposed that the contract is the most serious critical risk factor in IS projects, since the contract is the negotiation and enforcement tool used by all parties to convey their needs, concerns and relationships. The risks are particularly significant if the project scope is ill-defined or not firmly agreed between parties.

Any modifications or revisions of the project specifications after the contract are always to be considered as highly risky (Sumner, 2000; Kasser, 1998). Therefore, early negotiation of requirements is fundamental as proposed by Boehm *et al.* (1995). Furthermore, ill-defined or ambiguous requirement specifications are equally dangerous (Shull *et al.*, 2000), and likely to originate problems of usefulness and deviations from both timelines and budgets. These are well-known risks and identified even in the earlier days of computing as discussed by Bostrom and Heinen (1977). These were found to be a prevalent cause of failure by the analysis of the case-studies. In particular, these problems became apparent in the Integrated National Crime Information System (INCIS) project developed for the New Zealand Police. In this case, the results were catastrophic. The final information system produce was hopelessly inadequate:

> The scope of INCIS has never been satisfactorily addressed in the documentation. In the initial Information Systems Planning exercise the scope was defined as "intelligence within the Police". At no time were the boundaries set, or the role if INCIS defined and set in context within the Police.
>
> Subsequently, INCIS became an "information" rather than an "intelligence" system, radically affecting the scope of the project. There seems to be a great deal of confusion at even this broad-brush level of definition (Small, 2000, p. 33-4).

Cadle and Yeate (2001) claim that ambiguous roles of partners in project planning and scoping, as well as unclear relationships between these parties, should be considered as important risks. This research found clear evidence of these risks in most of the case-studies surveyed. This was particularly evident in the London Ambulance Service (LAS) – Finkelstein (1995) case study:

> The intention with the award of the contract to the SO [System Options Ltd] was for them as the lead contractor to take on the overall project management responsibility although there is no specific reference to this in the contract. This role later became ambiguous as SO struggled to manage their own input to the project and LAS became more responsible by default for project management. The suppliers are clear that it was in reality LAS,

> through the Director of Support Services and the contract analyst, who were providing project management.

These problems can be further compounded by internal political difficulties in the customer's organization as discussed in the next section. In terms of pre-project, some of these internal issues were crucial in all of the case-studies analysed. Lack of understanding of organisational politics, culture and internal relationships were found to create close to impossible problems. This confirms the findings of other researches, such as Nah *et al.* (2001) who suggest that top management support is needed throughout the implementation and top management needs to publicly and explicitly identify the project as a top priority. Kasser (1998) proposes that that lack of senior management support is one of top ten risks in this type of project.

Finally, in terms of pre-project, it is in the early project planning process that catastrophic risks are often ignored and not taken into account. Planning needs to account for adequate resources (funds, staff, equipment, etc.) and should precede the actual contract whenever possible. An important part of this early planning must also encompass the substitution of current systems and whenever necessary the interfacing with other systems. This was identified as a crucial risk factor in a number of case-studies, namely in the US Navy Enterprise Resource Planning (ERP) project:

> DOD's [US Department of Defence] past history of not implementing systems on time and within budget. The project faces numerous significant challenges and risks that must be dealt with as the project moves forward. For example, 44 system interfaces 6 with other Navy and DOD systems must be developed and implemented. Long-standing problems regarding the lack of integrated systems and use of nonstandard data within DOD pose significant challenges and risks to a successful Navy ERP interface with these systems (GAO, 2005).

In fact, the majority of failure causes identified in the case-studies could have been avoided if careful planning would have done before the contract. The contract needs to be suitable for the specific project with clearly defined payment schedule and backup plans in case of delays and other unexpected emergencies. Additionally, a clear business plan and vision is required to steer the direction of the project and enable efficient monitoring throughout its life-cycle. These findings confirm a widely accepted view in the literature that a good plan should follow a sound business case based on a clear understanding of both long-term strategic and short-term tangible benefits. In accordance to this business case, planning should provide for efficient use resources, monitoring of costs, assessment and mitigation of risks and the adherence to sound quality standards.

3.2 Customer

Customers are not always familiar with modern information and communication technology and their inherent affordances and risks. This may result in undue optimism and overambitious expectations by customers, which may result in overambitious requirement specifications and unwillingness to accept the final system after development. This was a recurrent theme in all the case-studies surveyed and a reality even in organisations with a long tradition of in-house IS design and development. This issue has long been recognised in the literature and Kirk and Vasconcelos (2003) found that negotiating through the client system and the

codification of the risk assessment process in relationship to the client itself were explicitly presented as a fundamental area of activity of management consultancies involved in the implementation of information technology (IT) projects. In the same study, these authors found that conversely, these were areas far less explicitly addressed by technology consultancies involved in similar projects. Authors, such as Lyytinen (1988) propose that stakeholders' expectation of failure is a gap between stakeholders' perceptions of what the IS can do and the actual system performance. Additionally, as found in the majority of cases in this research, managers may be ill-equipped to take decisions in relation to technology, but at the same time strongly pressured to succeed. This combination may have dramatic effects as can verified in the LAS failure report:

> An important factor was almost certainly the culture within the LAS of "fear of failure". Given the management changes of the last two years senior management were continually under pressure to succeed. This may have put undue pressure on management directly concerned with CAD [Computer-aided Design] to ensure that the system was implemented to timetable and to budget. This may have blinded them to some of the fundamental difficulties with the system that perhaps in retrospect seem rather more obvious (Finkelstein, 1995).

Furthermore, the internal constitution and politics of the customer may represent result in another important subset of risks. IS projects require full cooperation from all involved parties. Conflicts between user departments and internal political difficulties can bring conflict of interests to the surface and create great difficulties to IS functional analysis, design and testing, as well as, final acceptance. Risks emerging from these internal realities where apparent throughout the analysis, particularly in highly complex organisations such as US Department of Defence (DOD):

> Until DOD develops and implements an effective strategy for overcoming resistance, parochialism, and stovepiped operations, transformation efforts, as envisioned by the 1995 task force report, will not be successful and the department will be faced with the continued proliferation of numerous business systems that are nonintegrated, duplicative, and waste limited resources (GAO, 2006).

Furthermore, projects that may lead to a significant change in organizational structure and culture may result in strong user resistance and cause a series of risks. Managers on the customer side have therefore a very crucial role mediating and negotiating this change, as well as preparing the organisation to accept the new system.

3.3 Project management

Poor project management is universally accepted as a major cause of risk and failure in IS projects. The literature in the field is very rich and exhaustive. The results of this analysis seem to confirm the vast majority of theoretical assertions by authors in the field. This study identified risks around three main areas: human resources, project planning and project monitoring and reporting.

Deficiencies in project planning and team building are well-known risk factors (Kasser, 1998). Cadle and Yeate (2001) suggest that a full and complete project plan may not necessarily be presented before the contract but a comprehensive and proper project management strategy needs to be initiated as soon as possible. Furthermore, a well-balanced team including both well and less experienced analysts and SW

developers needs to be built. Finally, efficient communication channels linking project managers, project team, customer managers and end-users the essential to ensure flows of information and feedback. These communication channels are viewed as the key of final success in IS development and implementation (Cadle and Yeate, 2001). Finally, the plan should include formally defined and agreed milestones and deliverables (Holland and Light, 1999). These milestones and timelines enable appropriate project monitoring and control, as well as timely mitigation decisions whenever risk events emerge. Management of these deadlines needs to be met in order for the project to stay within agreed schedules and budgets and to maintain project team credibility.

More interestingly, this research identified that it was in reporting and documenting project progress that the majority of public sector managers failed. This may have been due to prevalent public sector cultures, or just lack of specific training for IT project management roles:

> Tracking, as applied by best practices in this area, is used to measure, identify, and report on the health of a project's schedule and cost, as these relate to work products, critical events, and other project commitments. However, we found that at SBA [Small Business Administration] project management reports were not always available and, when available, lacked comparative data for analysis. In addition, recording and reporting of project information either did not occur, or were inconsistently performed (GAO, 2000).

Project management remains, however, an umbrella term for many elements involved in systems failure. Therefore, technological and methodological problems are often misunderstood or confused with project management.

3.4 Technological issues

Similarly with project management issues, technological causes of failure have been debated in the field of IS since its early beginnings. Also in this case, most of these study's findings are in accordance with the very exhaustive and extensive literature in technology risk factors. The study identified both stability and compatibility of hardware (HW) and SW platforms as a major cause of problems. Furthermore, this survey shown that unproven or unfamiliar technologies may cause disappointment and lead to under-performance or conflicts with unrealistic expectations of technology. An excellent example emerged from the UK e-passport project:

> Current facial recognition technology is not reliable enough to enable the automated checking of applications against the full database of existing passport holders although the Identity and Passport Service is piloting its use on a smaller scale (NAO, 2007).

However, the study also confirmed that risks lie also with the technological development infrastructure, namely with unknown or unfamiliar programming languages, development tools and even development methods.

3.5 Development methodology

Methodological problems have often been confused with project management. In fact, these are very separate issues. Different design and development methodologies may result in very different project structures and risks. There are well-known differences between agile and structured methodologies, with defenders of both approaches engaging in fierce discussions and theoretical arguments. For the practitioner,

however, these differences are more then theoretical and hypothetical. As identified in this study, choosing a methodology out of fashion or positioning in the field, may bring severe risks to the project and increase probability of delays and budget overruns.

In general, terms, a classical definition of an IS project may comprise the well-accepted phases of systems analysis, systems design, system development and testing, system installation and systems maintenance.

One of the persistent oversights of IT practitioners and programmers is usually the systems analysis stage of IS projects. Concentration in technical concerns of design and programming has systematically led reductionist interpretations of requirements, functional specifications, end-user needs and organisational constraints. This technological induced blindness is persistent in the SW sector is still prevalent today. In fact, the lack of user consultation and holistic awareness of organisational needs was found to be one of the critical failure factors in most of the case-studies surveyed:

> NASA [National Aeronautics and Space Administration] did not consider the information needs of key system users and deferred addressing the requirements of program managers, cost estimators, and the Congress. Although this module should eliminate NASA's separate, incompatible accounting systems, little has been done to reengineer acquisition management processes (Integrated Financial Management Program (IFMP) NASA – GAO, 2003).

Similarly, system designing, as the next step, is carried often out on the basis that a full comprehension of organization background and requirements has been achieved. This stage requires constant communicating within the project team as well as between the project team and the customer. Design ranging from the overcomplicated to the reductionist may have profound implications in the success of IS projects. In order to ensure that the project team is producing what the customer requires, it is a good strategy to have customer's agreement on designs and prototypes before the starting heavy processes of programming. Again in this case, the lack of consultation with the customer may lead to significant needs form actual requirements and decrease chances of acceptance of the final system:

> A broader challenge and risk that is out of the Navy ERP project's control, but could significantly affect it, is DOD's development of a BEA [Business Enterprise Architecture]. As we recently reported, 51 DOD's BEA still lacks many of the key elements of a well-defined architecture and no basis exists for evaluating whether the Navy ERP will be aligned with the BEA and whether it would be a corporate solution for DOD in its "To Be" or target environment (US Navy ERP – GAO, 2005).

Systems development and testing is probably the more critical phase of any IS project. Adequate programming and testing methods and techniques need to be adopted. The use of unstable and sometimes incompatible SW and HW platforms may represent a significant risk for the project. More importantly, the use of emergent fashions and sometimes unproven methods and tools may result in easily predictable risks and slippages in timelines and budgets:

> The decision to use OOT [Object Oriented Technology] made the implementation of the INCIS application high risk because it was very new technology and standards were immature. At the date of Contract, there were some specialised applications such as Graphical User Interfaces (GUI) using objects. However, at that stage, there were few commercial

> applications of the size and complexity of the planned INCIS application using an OOT, especially in a distributed Object Oriented (OO) client/server environment. The methodologies and support tools for designing and developing business systems using an OOT were not readily available nor was there a pool of experienced developers (INCIS – Small (2000, p. 33-4).

Finally, it was found in almost all cases that the lack of a thorough and inclusive testing strategy is an unacceptable risk and one of the major causes for disaster:

> DTS development and implementation have been problematic, especially in the area of testing key functionality to ensure that the system will perform as intended. Consequently, critical flaws have been identified that resulted in significant schedule slippages between the planned and actual system deployment (DOD DTS – GAO, 2006).

4. Conclusions

The checklist presented in this paper aims at supporting both practitioners and researchers in their risk thinking and assessment. For practitioners, the checklist is an important decision-making support tool and is aimed at helping in risk identification and assessment activities. For researchers, on the other hand, the check list provides a first attempt at establishing an risk ontology and a point of departure for further research. Future research in this area should aim at completing this first proposal, but also linking these risk factors to both causes and consequences.

Another major conclusion of the case-study survey is that a considerable amount of risk factors are clearly incurred even before the start of the formal project. All these factors, identified in the pre-project dimension, severely pre-determine the future of the project and create very predictable risks that could be avoided if given due consideration. In fact, this research found evidence that risk thinking should start very early as part of pre-project and not, as most of the modern design and development methodologies propose, solely as part of the development process itself. For instance, dynamic systems development method proposes risk thinking as part of the functional model iteration, rational unified process proposes risk analysis and assessment as part of the inception phase, and finally, even extreme programming a proclaimed risk-driven approach (Li *et al.*, 2006) only really formally advocates risk thinking during release planning. It is clear from findings of this study that risk thinking must start long before this, in fact, long before contracts are established.

The usefulness of a checklist as the one proposed may be questioned if the list is used monolithically and never improved. In fact, "as nothing is staying stable in our world, having a generic list is a drawback, unless it is being updated constantly" (Vidalis, 2003, p. 20). Therefore, this list is expected to undergo a process of co-evolution with practice. It is not expected to be the definite and comprehensive response to every conceivable present and future risk event, but a starting point for risk assessment.

Finally, it is important to highlight that this paper has focused on the pre-implementation and implementation phases of IT/IS projects, but other studies (Brown, 1995, 1998; Doolin, 2004; Vasconcelos, 2007) point towards the occurrence of significant risks in the post-implementation and exploration phases of the IS life-cycle. Further research into IS post-implementation should focus on negotiated interactions

between social actors and technologists, in order to fulfil often divergent organisational internal agendas. This is an area where there is a significant gap, particularly in the relationships between risk thinking, development methodologies and agency in action.

References

Alavi, M. and Carlson, P. (1992), "A review of MIS research and disciplinary development", *Journal of Management Information Systems*, Vol. 8 No. 4, pp. 45-62.

Bhandari, P., Nunes, M. and Annansingh, F. (2005), "Analysing the penetration of knowledge management practices in organisations through a survey of case studies", *Proceedings of the 4th European Conference on Research Methodology for Business and Management Studies (ECRM 2005), Université Paris Dauphine, Paris, France*, April 21-22, pp. 37-45.

Boehm, B., Bose, P., Horowitz, E. and Lee, M. (1995), "Software requirements negotiation and renegotiation aids: a theory-W based spiral approach", *International Conference on Software Engineering. Proceedings of the 17th International Conference on Software Engineering, 1995, Seattle, WA, USA*, pp. 243-53.

Bostrom, R. and Heinen, J. (1977), "MIS problems and failures: a socio-technical perspective. Part 2: the application of socio-technical theory", *MIS Quarterly*, Vol. 1 No. 4, pp. 11-28.

Bronte-Stewart, M. (2005), "Developing a risk estimation model from IT project failure research", *Computing and Information Systems Journal*, Vol. 9 No. 3, available at: http://cis.paisley.ac.uk/research/journal/V9/V9N3/failure.doc (accessed March 14, 2007).

Brown, A. (1995), "Managing understandings: politics, symbolism, niche marketing and the quest for legitimacy in IT implementation", *Organisation Studies*, Vol. 16 No. 6, pp. 951-69.

Brown, A. (1998), "Narrative, politics and legitimacy in an IT implementation", *Journal of Management Studies*, Vol. 35 No. 1, pp. 35-58.

Brown, M. (2000), "Mitigating the risk of information technology initiatives: best practices and points of failure for the public sector", in Garson, G. (Ed.), *Handbook of Public Information Systems*, Marcel Dekker, New York, NY, pp. 153-64.

Bryman, A. (2002), *Research Methods and Organisation Studies*, Routledge, London.

Cadle, J. and Yeate, D. (2001), *Project Management for Information Systems*, Financial Times/Prentice-Hall, Harlow.

Chapman, C. and Ward, S. (1997), *Project Risk Management: Processes, Techniques and Insights*, Wiley, New York, NY.

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

Clegg, C., Axtell, C., Damadoran, L., Farbey, B., Hull, R., Lloyd-Jones, R., Nicholls, J., Seell, R. and Tomlinson, C. (1997), "Information technology: a study of performance and the role of human and organizational factors", *Ergonomics Journal*, Vol. 40 No. 9, pp. 851-71.

Doolin, B. (2004), "Power and resistance in the implementation of a medical management information system", *Information Systems Journal*, Vol. 14, pp. 343-62.

Drori, O. (1997), "From theory to practice or how not to fail in developing information systems", *Software Engineering Notes*, Vol. 22 No. 1, pp. 85-7.

Drucker, P. (1975), *Management: Tasks, Responsibilities, Practices*, W. Heinemann, Ltd, London.

Dvir, D., Lipovetsky, S., Shenhar, A. and Tishler, A. (1998), "In search of project classification: a non-universal approach to project success factors", *Research Policy*, Vol. 27 No. 9, pp. 915-35.

Easterby-Smith, M. (2002), *Management Research: An Introduction*, Sage, London.

Fielding, R. (2002), "IT projects doomed to failure", *VNUNET.COM News*, November, available at: www.vnunet.com/vnunet/news/2120858/projects-doomed-failure (accessed March 14, 2007).

Finkelstein, A. (1995), "Report of the inquiry into the London Ambulance Service", available at: www.cs.ucl.ac.uk/staff/A.Finkelstein/las/lascase0.9.pdf (accessed March 14, 2007).

GAO (2000), "Information technology management: SBA needs to establish policies and procedures for key IT processes", available at: www.gao.gov/archive/2000/ai00170.pdf (accessed March 14, 2007).

GAO (2003), "Business modernization: improvements needed in management of NASA's integrated financial management program", available at: www.gao.gov/new.items/d03507.pdf (accessed March 14, 2007).

GAO (2005), "DOD business systems modernization: navy ERP adherence to best business practices critical to avoid past failures", available at: www.gao.gov/new.items/d05858.pdf (accessed March 14, 2007).

GAO (2006), "DOD business transformation: defense travel system continues to face implementation challenges", available at: www.gao.gov/new.items/d0618.pdf (accessed March 14, 2007).

Gill, J. and Johnson, P. (1991), *Research Methods for Managers*, Paul Chapman, London.

Glesne, C. and Peshkin, A. (1992), *Becoming Qualitative Researchers*, Longman, New York, NY.

Harrin, E. (2007), "Between a rock and a hard place", *IT Now*, Vol. 49 No. 1, pp. 6-8.

Holland, C. and Light, B. (1999), "A critical success factors model for ERP implementation", *IEEE Software*, Vol. 16 No. 3, pp. 30-6.

Hood, C. and Rothstein, H. (2000), "Business risk management in government: pitfalls and possibilities", Centre for Analysis of Risk and Regulation at the London School of Economics and Political Science (CARR) Discussion Paper No. 0, available at: www.lse.ac.uk/collections/CARR/pdf/Business_Risk_Management_in_Govt.pdf (accessed March 14, 2007).

Hughes, B. and Cotterell, M. (2002), *Software Project Management*, McGraw-Hill, London.

Jackson, P. (1994), *Desk Research, Market Research Series*, Kogan Page, London.

Jalote, P. (2002), *Software Project Management in Practice*, Addison-Wesley Professional, Boston, MA.

Jaques, R. (2004), "UK wasting billions on IT projects", *VNUNET.COM News*, April, available at: www.computing.co.uk/vnunet/news/2124833/uk-wasting-billions-projects (accessed March 14, 2007).

Kasser, J. (1998), "What do you mean you can't tell me if my project is in trouble?", *Proceeding of the First European Conference on Software Metrics (FESMA 98), Antwerp, Belgium*.

Keil, M., Cule, P., Lyytinen, K. and Schmidt, R. (1998), "A framework for identifying software project risks", *Communication of the ACM*, Vol. 41 No. 11, pp. 76-83.

Kirk, J. and Vasconcelos, A. (2003), "Management consultancies and technology consultancies in a converging market: a knowledge management perspective", *Electronic Journal of Knowledge Management*, Vol. 1 No. 1, pp. 33-46.

Kliem, R. and Ludin, I. (2000), *Reducing Project Risk*, Gower Publishing Limited, Aldershot.

Lawrence, M. (2003), "Are you up to it?", *The Computer Bulletin for Information Systems Professionals*, Vol. 45 No. 2, pp. 22-3.

Li, M., Huang, M., Shu, F. and Li, J. (2006), "A risk-driven method for extreme programming release planning", *International Conference on Software Engineering. Proceeding of the 28th International Conference on Software Engineering, Shanghai, China*, May 20-28.

Lyytinen, K. (1988), "Expectation failure concept and system analysts' view of information system failures: results of an exploratory study", *Information & Management*, Vol. 14 No. 1, pp. 45-56.

Mantel, S., Meredith, J., Shafer, S. and Sutton, M. (2001), *Project Management in Practice*, Wiley, New York, NY.

Nah, F., Lau, J. and Kuang, J. (2001), "Critical factors for successful implementation of enterprise systems", *Business Process Management Journal*, Vol. 7 No. 3, pp. 285-96.

NAO (2007), "Identity and passport service: introduction of e-passports", available at: www.nao.org.uk/publications/nao_reports/06-07/0607152.pdf (accessed March 14, 2007).

Nunes, M. and Annansingh, F. (2002), "The risk factor", *The Journal of the Institute for the Management of Information Systems*, Vol. 12 No. 6, pp. 10-12.

Orlikowski, W. and Baroudi, J. (1991), "Studying information technology in organizations: research approaches and assumptions", *Information Systems Research*, Vol. 2 No. 1, pp. 1-28.

Pressman, R. (1997), *Software Engineering: A Practitioner's Approach*, 4th ed., McGraw-Hill, New York, NY.

Pritchard, C. (2004), *The Project Management Communications*, Toolkit Artech House, London.

Remenyi, D., Williams, B., Money, A. and Swartz, E. (1998), *Doing Research in Business and Management: An Introduction to Process and Method*, Sage, London.

Saunders, M., Lewis, P. and Thornhill, A. (2000), *Research Methods for Business Students*, Pearson Education Limited, Harlow.

Shull, F., Rus, I. and Basili, V. (2000), "How perspective-based reading can improve requirements inspections", *Computer*, Vol. 33 No. 7, pp. 73-9.

Small, F. (2000), "Ministerial inquiry into INCIS", available at: www.justice.govt.nz/pubs/reports/2000/incis_rpt/INCIS%20inquiry.pdf (accessed March 14, 2007).

Stufflebeam, D. (2000), "Guidelines for developing evaluation checklists: the checklists development checklist (CDC)", available at: www.wmich.edu/evalctr/checklists/guidelines_cdc.pdf (accessed March 12, 2007).

Sumner, M. (2000), "Risk factors in enterprise wide information management systems projects", *Special Interest Group on Computer Personnel Research Annual Conference Proceedings of the 2000 ACM SIGCPR Conference on Computer Personnel Research, 2000, Evanston, IL*, pp. 180-7.

Taylor, J. (2003), *Managing Information Technology Projects: Applying Project Management Strategies to Software, Hardware and Integration Initiatives*, American Management Association, New York, NY.

Tsui, F. (2004), *Managing Software Projects*, Jones and Bartlett Publishers, Sudbury.

Vasconcelos, A. (2007), "The role of professional discourses in the organisational adaptation of information systems", *International Journal of Information Management*, Vol. 27 No. 4, pp. 279-93.

Vidalis, S. (2003), "A critical discussion of risk & threat analysis methods & methodologies", School of Computing Technical Report CS-04-03, School of Computing, University of Glamorgan, Wales, available at: www.comp.glam.ac.uk/staff/svidalis/Technical%20Reports/Threat%20&%20Risk%20TR.doc

Voyages (1996), "Unfinished voyages, a follow up to the CHAOS report", The Standish Group, available at: www.standishgroup.com/sample_research/unfinished_voyages_1.php (accessed March 12, 2007).

Walliman, N. (2001), *Your Research Project: A Step by Step Guide for the First Time Researcher*, Sage, London.

Whittaker, B. (1999), "What went wrong? Unsuccessful information technology projects", *Information Management & Computer Security*, Vol. 7 No. 1, pp. 23-9.

Yin, R. (1984), *Case Study Research: Design and Methods*, Sage, Beverly Hills, CA.

Appendix

(The Appendix follows overleaf.)

Appendix

Table AI.
A proposition of an information systems project risk checklist

Project risk dimensions	ID	Risk factors
Pre-project		
Requirement specification and project scoping	1	Requirement specifications are ill-defined
	2	Requirement specifications are ambiguous
	3	Project scope and objectives are inappropriately defined
	4	Requirement specifications are incomplete
	5	Lack of early negotiation with customer and users
Contractual relationships	6	Complex and unclear relationships between partners, customers and suppliers
	7	Ambiguous roles of partners in project planning and scoping
	8	Disagreement between involved partners
	7	Unclear payment schedule or a fixed-price contract
	8	Inappropriate selection of suppliers due to ambiguous selection criteria
	9	Uncertain long-term partnership between the customer and the supplier after the project
Project planning	10	Deficient planning and resource allocation
	11	Lack of previous experience by the customer
	12	Lack of clear definition of development methodologies or/and technological infrastructures
	13	Lack of planning for replacement of current systems or/and interfacing with current systems
	14	Lack of backup plan for delays or/and under-performance of new system
	15	Lack of a quality control system before project
Organisational environment	16	Inadequate current business processes for IS implementation
	17	Significant need for re-engineering of current business processes
	18	Inappropriate business plan and IS vision
	19	Lack of senior management support or/and internal political resistance
	20	Lack of understanding of customer's organizational culture
	21	Requirement for widespread and persistent organizational culture change
	22	Potential for end-user resistance
	23	Lack of capability to identify and/or absorb both external and internal uncertainties

(*continued*)

Table AI.

Project risk dimensions	ID	Risk factors
Customer		
Internal and external environment	1	Conflicts between user departments
	2	Constant external pressure and uncertainty on how to manage it
	3	Inefficient communication between all involved parties
	4	Internal political difficulties
	5	Lack of confidence on the project by the internal users
	6	Mistrust between management and staff
	7	Difficulties in harmonizing different and sometimes conflicting internal user's perspectives on the project
End-user	8	Target users are unfamiliar with the technology and require additional training
	9	Lack of end-user support
	10	End-user reluctance in changing or even accepting the new system
Management	11	Lack of understanding of technical issues and functional scope by management
	12	Lack of information and IT skills by management
	13	Internal resources and access are not adequately provided to the project team
Project management		
Human resource	1	Reluctance by the customer to attend project meetings
	2	Inappropriate staffing and/or personnel shortfalls
	3	Inappropriate project team structure
	4	Inexperienced team members in core business or technology project components
	5	Lack of clear processes of accountability and responsibility
	6	Lack of commitment to the project by team members
	7	Inadequate balance of junior and senior staff in the project team
Project planning	8	Lack of effective processes of estimation
	9	Lack of effective quality control and assurance according to agreed standards
	10	Ill-definition of milestones and related deliverables
	11	Ineffective risk identification and assessment
	12	Ineffective planning for risk mitigation and/or avoidance
	13	Lack of clear project management structure and methodology
Project monitoring and reporting	14	Inappropriate project reporting
	15	Unrealistic monitoring of timeliness and budgets

(*continued*)

Table AI.

Project risk dimensions	ID	Risk factors
	16	Ineffective risk monitoring according to contract, requirement specifications, time boxes and prioritization of features
	17	Inappropriate human resource management
	18	Lack of leadership and/or motivating attitudes by project managers
Technological issues		
IS infrastructure and base technologies	1	Emerging or unproven technologies
	2	Incompatible technologies with project constraints and/or requirements
	3	Erroneous, ambiguous or incomplete technology feasibility studies
	4	Unfamiliar technologies to the design and development team
	5	Unstable or incompatible HW infrastructures and platform
Development technologies	6	Emerging or unproven programming and debugging technologies
	7	Overly complex or time demanding programming and debugging technologies
	8	Unfamiliar development environment to the project team
Development methodology		
General methodological issues	1	Use of emerging, unproven and often misunderstood methodologies
	2	Use of inadequate or reductionist methodologies
	3	Adoption of technologically centric design and development approaches
	4	Adoption of non-comprehensive (not fully covering the entire process) methodologies
	5	Project managers that do not fully understand the technical requirements of an IS project
	6	Inadequate planning for social-technical systems design and development
Systems analysis	7	Inadequate comprehension of the current system and current situation of the organization
	8	Misunderstanding of user requirements
	9	Interpretation of end-user requirements from a reductionist technological perspective
	10	Lack of an integrative holistic perspective of organisational needs
	11	Inadequate prioritisation and assessment of requirements, functionalities and features
	12	Poor dialogue, negotiation and communication with the end-users and the organisation in general
System design	13	Poor dialogue between designers and analysts
	14	Poor dialogue between designers and end-users
	15	Overcomplicated designs that may result in system extremely heavy and complex systems
	16	Non-use of prototyping to negotiate design solutions with the customer
	17	Non-compliance with prioritization and specifications agreed in previous stages
	18	Designs emerging out of fashion or current trends rather then explicit needs

(*continued*)

Project risk dimensions	ID	Risk factors
System development and testing	19	Poor dialogue between designers and programmers
	20	Attempt to produce a complete and perfect system in one go
	21	Unstable and/or incompatible SW and HW system platforms
	22	Initiate programming before design is fully agreed and/or complete
	23	System testing without final user involvement
	24	Inadequate testing the final integrated system before final implementation
	25	Programming without agreed communication channels between programmers
	26	Programming without agreed information sharing channels between programmers
	27	Programming without agreed processes for sharing and re-use of common code between programmers
	28	Code emerging out of fashion or current trends rather then explicit needs
	29	Programmer-oriented coding instead of user-oriented
System installation	30	Lack of planned and agreed systems installation and cutover processes
	31	Lack of a user training plan and insufficient user training before installation
	32	Initiate training without complete testing
System maintenance	33	Lack of a clear and agreed maintenance plan
	34	Assignment of unqualified staff for systems administration and maintenance

Table AI.

Table AII.
List of case-studies

ID	Title	Organization	Reporting organization	Year	URL
1	ERP in Public School District	The San Diego Public School District	Kellogg School of Management Northwestern University	2002	www.kellogg.northwestern.edu/faculty/jeffery/htm/cases/SDSU%20Case%20wm.pdf
2	Integrated Financial Management Program (IFMP)	NASA	United States General Accounting Office	2003	www.gao.gov/new.items/d03507.pdf
3	The National Program for IT in the NHS	Department of Health, UK	National Audit Office, UK	2006	www.nao.org.uk/publications/nao_reports/05-06/05061173.pdf
4	Navy ERP	Department of Defense, US	United States General Accounting Office	2005	www.gao.gov/new.items/d05858.pdf
5	Defense Travel System (DTS)	Department of Defense, US	United States General Accounting Office	2006	www.gao.gov/new.items/d0618.pdf
6	IT Investment Management (ITIM)	Bureau of Land Management	United States General Accounting Office	2003	www.gao.gov/new.items/d031025.pdf
7	Information Technology Management	Small Business Administration	United States General Accounting Office	2000	www.gao.gov/archive/2000/ai00170.pdf
8	Identity and Passport Service: Introduction of ePassports	The Identity and Passport Service; UK Office	National Audit Office, UK	2007	www.nao.org.uk/publications/nao_reports/06-07/0607152.pdf
9	Integrated National Crime Information System (INCIS)	New Zealand Police	Ministry of Justice	2000	www.justice.govt.nz/pubs/reports/2000/incis_rpt/INCIS%20inquiry.pdf
10	London Ambulance Service (LAS)	National Health Service (NHS)	South West Thames Regional Health Authority	1995	www.cs.ucl.ac.uk/staff/A.Finkelstein/las/lascase0.9.pdf