Risk Factors of Large Internal Information Systems Projects in Government

Euripidis Loukis
University of the Aegean, Greece

Yannis Charalabidis
University of the Aegean, Greece

ABSTRACT

Government organizations attempt to develop large internal information systems (IS) in order to support their lengthy and complex internal processes, enable citizens' e-transactions and in general promote e-government. However they experience high failure rates, resulting in waste of considerable financial resources and loss of significant opportunities. This chapter presents an empirical study of the risk factors of large internal IS projects in government, based on the analysis of 80 Official Decisions of the Greek Government Information Technology Projects Advisory Committee. This analysis reveals 21 risk factors, which are discussed and categorized with respect to their origin in order to understand better the sources of this risk. Behind these risk factors some political factors have been distinguished, which are associated with intra- and inter-organizational politics and competition. Also, the identified risk factors are compared with the ones found in other similar studies. Based on the findings of this study implications/recommendations for politicians and managers of the public sector have been formulated.

INTRODUCTION

Government organizations attempt to develop large internal information systems (IS), either bespoke or based on existing enterprise resource planning (ERP) packages (usually with appropriate modifications/adaptations), in order to support their internal processes, enable citizens' e-transactions and in general promote e-government. While the main focus of most countries' e-government programs is the development of 'extrovert' e-transaction IS, which allow citizens and firms to conduct transactions with government organizations through electronic networks (e.g. Internet or mobile phones), their efficiency relies strongly on the existence of sufficient internal IS infrastructures supporting the quick and complete processing of these e-transactions. Many of these internal IS have to be large and complex, due to the big size of the government organizations and the complexity of their processes. However, these ambitious IS development projects have high complete or partial failure rates (i.e. high rates of abandonment or completion with significantly lower technical performance, functionality and business benefits), resulting in waste of considerable public financial resources and loss of significant opportunities (Poulymenakou & Holmes, 1996; Cabinet Office, 2000; Heeks, 2003; OECD, 2001 and 2003; Gauld, 2007; Goldfinch, 2007). OECD (2001, 2003) regards these failures as 'the Hidden Threat to E-Government' and concludes that unless governments learn to manage the risks connected with large IS projects, their 'e-dreams' will turn into 'global nightmares'. Therefore for the advancement of e-government it is necessary to identify and understand the risk factors of the large internal IS projects in government and to design appropriate strategies for managing and addressing them in order to reduce their risk and failure rates.

It should be noted that similar problems are experienced by private sector firms as well (Standish Group, 1995, 2001, 2004; Drummond, 1996; Dalcher & Genus 2003; Goulielmos, 2005; Fitzgerald & Russo, 2005; Bharadwaj et al, 2009; Loukis et al, 2011), indicating that large IS development is an inherently risky undertaking. For instance, the well known and widely quoted CHAOS Report (Standish Group, 1995) by the Standish Group reports that private sector software projects are 'in chaos': 31.1% of them are abandoned during the development cycle, while 52.7% of them, although they are completed and become operational, suffer serious budget overruns and/or schedule slips and/or offer less functionality and features than initially specified, while only 16.2% of them are finally successful; the subsequent versions of this Report found only small improvements of these failure rates (Standish Group, 1995). Bharadwaj et al (2009) from an empirical study conclude there are many IS failures in the private sector firms traded in stock exchanges, which result in significant abnormal drops of their stock prices and decline of their market value.

However, as described in the following 'Background' section in more detail, previous literature is dealing mainly with the risk factors of IS projects in private sector firms, and recently focuses on software development projects. Taking into account the fundamental differences between public and private sector organizations, which have been extensively analyzed and emphasized in the relevant previous literature (no market competition, short term goals set by political agendas and changing frequently, lengthy and complex internal processes, extensive legal framework defining fully all aspects of their operations, silo mentality of departments and limited cooperation among them, lower motivation by employees, avoidance of innovation mentality) (Bozeman and Bretschneider, 1986; Caudle, 1991; Heintze and Bretschneider, 2000; Wright, 2001; Boyne, 2002; Barton, 2006; Kraemer and King, 2006; Buelens and Van den Broeck, 2007), it is necessary to conduct further research in this area focused on the risk factors of government IS projects and covering the whole range of their activities (and not only software development). In this direction this study aims to investigate empirically the risk factors of the large internal IS projects in government, based on a big sample of such projects implemented in the Greek public sector, and to understand the main sources of this risk. We expect that the findings will be quite interesting and useful to researchers, practitioners, professional societies, educational institutions and consulting companies dealing with the areas of public administration and IS.

In the following section the background of this study is presented concerning previous research on the risk factors of IS projects. Then the research method and data are described, followed by the results with respect to the main risk factors. Next these risk factors are analyzed and categorized in order to understand the basic origins of risk and finally compared with the ones found by other similar studies. In the last section the conclusions, implications and directions for future research are outlined.

BACKGROUND

There has been extensive research for more than 30 years for understanding and reducing the high failure rates of IS projects, due to their high financial and non-financial costs. The main objectives of this research have been the identification of their main risk factors, defined as conditions that can present serious threats to the successful completion of an IS project within budget and schedule (Schmidt et al, 2001), the assessment of the risks they create and the development of strategies for managing them.

A first research stream aims to investigate in various levels of detail the risk factors of IS projects in general, without focusing on particular types of IS projects; there are some studies at a higher level attempting to identify the main groups or sources of risk factors, while some others go into more detail attempting to identify the particular risk factors in order to provide direct assistance to IS project managers (Zmud, 1979; Lucas, 1981; McFarlan, 1981; Lyytinen & Hirschheim, 1987; Willcocks and Margetts, 1993; Saarinen & Vepsalainen, 1993; Lai & Mahapatra, 1997; Jiang & Klein, 1999; OECD, 2001, 2003; Heeks, 2003; Royal Academy of Engineering and the British Computer Society, 2004; Gauld, 2007; Goldfinch, 2007; Bharadwaj et al, 2009). Most of this research is focused on the private sector IS. McFarlan (1981) concluded that the most important factors that affect the risk of an IS project are the size of the project, the experience of the project team with the ICTs used in this project and also the level of structure of the project (a highly structured IS project with predefined outputs agreed by the users and not subject to change during the lifecycle of the

project has less risk). Willcocks and Margetts (1993) work at a higher level and finally group the risk factors of IS projects into four categories as to their source/origin, which are associated with the outer context, the inner context, the content and the process of the project respectively. Jiang & Klein (1999) investigate the relationship between the ten most important IS projects risk factors according to the literature (technological newness, project size, lack of team's general expertise, lack of team's expertise with the task, lack of team's development expertise, lack of user support, insufficient resources, lack of clarity of roles definitions, application complexity and lack of user experience) and four measures of IS project success; they concluded that each of the investigated success measures is affected by a different set of risk factors. Dalcher & Genus (2003) from a synthesis of the conclusions of the papers included in a special issue on this topic identify a number of critical issues, which if not appropriately managed can lead to IS projects failure: users involvement, expectations management and adaptive attitude to learning and change, vendor relationship management, cooperation among stakeholders and appropriate risk management.

On the contrary only a small part of this research stream is dealing with the risk factors of the public sector IS projects. One of the few empirical studies on this topic has been conducted by OECD (2001), concluding that governments face big problems and failures when implementing large IS projects, and identifying a set of basic risk factors of these projects: large size, limited involvement of end-users, inappropriate governance structures, limited attention to business process change, use of emerging and immature technologies, weaknesses in managing relationships with external vendors, lack of specialized and knowledgeable human resources, weaknesses in project management and risk management and lack of accountability of business management. Also, some interesting case studies have been conducted of partially or totally failed IS projects in the public sector, which offer insight into the main risk factors that caused failure. For instance, Gauld (2007) analyzes the failure and abandonment of a large IS project in a public New Zealand hospital and concludes that, in addition to the risk factors found in private sector IS projects, the ones of public sector face additional unique political and organizational risk factors, which increase failure rates.

Gradually the IS practitioners' and researchers' community realized that the most complex, difficult and risky part of an IS project (i.e. the one with the highest probability of complete or partial failure) is the software development, giving rise to a second research stream focusing on the risk factors of the software development (sub)projects (Boehm, 1991; Keil et al, 1998; Schmidt et al, 2001; Barki et al, 2001; Walace et al, 2004a and 2004b; Han & Huang, 2007). While the first research stream identified the most important factors that give rise to threats to the successful completion of an IS project as a whole, it was an imperative to examine how important these 'generic' risk factors are for the highly complex and difficult software development part of the project in particular, and whether there are additional risk factors 'specific' to software development that give rise to significant threats to its successful completion. From this research stream it is worth mentioning an international study of software development projects risk factors presented by Keil et al (1998) and Schmidt et al (2001). It was based on three simultaneous 'ranking - type' Delphi surveys conducted in three different cultural settings: in USA, Finland and Hong Kong. It concluded that risk factors change with time and also depend highly on the cultural, socioeconomic and organizational context. However, it identified eleven risk factors, which were common to all three countries: lack of top management commitment to the project, failure to gain user commitment, misunderstanding the requirements, lack of adequate user involvement, lack of required knowledge/skills in the project personnel, lack of frozen requirements, changing scope/objectives, introduction of new technology, failure to manage end-user expectations, insufficient/inappropriate staffing and conflict between user departments. Han & Huang (2007) examine empirically the probability of occurrence and the impact on software projects success of six main risk dimensions, concluding that requirements risk has the highest probability of occurrence and also the highest impact on software project success.

From this literature review it has been concluded that a useful body of knowledge concerning the critical question of IS projects risk factors has been created. However, as mentioned above most of this research focuses on the private sector, and their conclusions - as mentioned in the Introduction - cannot be directly and automatically transferred to the public sector, due to the fundamental differences of the public organizations from the private ones. Furthermore, even this limited research that has been conducted concerning the risk factors of government IS projects has the form of case studies, and there is a lack of empirical research based on larger samples of public sector IS projects

which could provide more generalizable conclusions. Another interesting conclusion drawn from this literature review is that the most recent research on IS projects risk factors focuses mainly on software development projects and neglects the risk factors associated with the whole lifecycle of an IS project, which usually includes not only software development activities, but also many other types of risky activities as well (e.g. request for proposals documents preparation, contracts preparation, negotiation and management activities, hardware procurement activities, networks development activities, etc.) The present study contributes to filling these research gaps.

RESEARCH METHOD AND DATA

The research method we followed for identifying the risk factors of the large internal IS projects in government was based on the study and analysis of Official Decisions of the Greek Information Technology Projects Advisory Committee (ITPAC) and also on interviews with all its members. In Greece, all large government IS projects with a budget exceeding 1 million Euro have to be approved by the Minister of Interior, Public Administration and Decentralization. For this purpose the ITPAC has been established, which is a high-level scientific committee, consisting of highly respectable and experienced IS professionals, usually IS Directors of Ministries and University Professors in the area of IS or other relevant areas. For each large IS project the competent Ministry submits to ITPAC a predefined set of documents about it, which includes description of its current IS infrastructure and personnel, detailed functional and technical description of the project, detailed budget, implementation plan and analysis of all project activities, description of project team, request for proposals (RFP) document(s), proposed contract(s), etc. The ITPAC examines these documents, discusses them, interviews the project manager and finally prepares an proposal to the Minister of Interior, Public Administration and Decentralization concerning the approval or not of the project, and also a number of 'recommendations' concerning necessary modifications, corrective actions, etc.; each recommendation is a 'diplomatic' expression of a highly important risk factor in this project, which can have a negative impact on it if not properly managed.

In particular, the research method we followed in this study included the following six steps:

i. Initially, 80 ITPAC Official Decisions concerning large internal IS projects of various government organizations were studied and analyzed.
ii. Then, in-depth semi-structured interviews were conducted with all members of the ITPAC, in which they were asked to explain to us in detail the recommendations included in the above Official Decisions and the reasons and justifications behind each of them.
iii. A generalization and consolidation of the recommendations included in the above ITPAC Official Decisions followed, which was necessary because each of them was specialized for a particular project. Each author working separately grouped similar specialized recommendations into one consolidated recommendation and in this way finally produced a list of consolidated recommendations; then the results of the two authors were compared and differences were resolved.
iv. For each of these consolidated recommendations each author working separately determined the corresponding risk factor, taking also into account the explanations given by the members of the ITPAC in the interviews of the second step; the results of the two authors were compared and differences were resolved. In this way the list of consolidated recommendations and corresponding risk factors was finalized; then for each of them its relative frequency was calculated (indicating in what percentage of the 80 examined large IS projects this risk factor appears).
v. These risk factors were further analyzed and associated by both authors in cooperation with the particular characteristics of the public sector, based on the explanations given by the members of the ITPAC in the interviews of the second step.
vi. The above risk factors were categorized by both authors, using the framework of Willcocks and Margetts (1993) in order to identify the main sources of risk in the large government IS projects; the small differences were then resolved.

The research approach we adopted in the present study, based on the analysis of the Official Decisions of ITPAC, is similar to the typical 'Delphi surveys' frequently used by other studies (e.g. Schmidt et al, 2001), but offers significant advantages over it: the members of ITPAC have a much more serious,

professional and responsible involvement in the identification of the risk factors of IS projects (having to produce official documents on them) than the participants in a typical Delphi survey, who usually regard it as a 'research exercise' of minor importance for them. Also, the interaction among the members of ITPAC is much higher than the interaction among the participants in a typical Delphi survey. Furthermore, the 'open' research approach we adopted in this study offers significant advantages in comparison to the alternative approach of combining risk factors identified by previous relevant research, creating a consolidated list of risk factors, and then presenting it to experienced experts and asking them to rate the importance of each risk factor of this list (e.g. on a 10 point scale), which has been used by several similar studies. Such a research approach can result in missing significant risk factors, which are specific to the context under examination, but do not exist in the other contexts from which the consolidated risk factors list has been derived. The above approach is combined with qualitative research (Ragin, 1994; Maylor and Blackmon, 2005) based on in-depth semi-structured interviews with the ITPAC members.

RESULTS – RISK FACTORS

The consolidated recommendations and the corresponding risk factors identified in the abovementioned steps (iii) and (iv) are shown in Table 1, in order of relative frequency (showing in what percentage of the 80 examined large internal IS projects each of them appears). Also in the last column we can see their categorization made in the step (vi) based on the framework of Willcocks & Margetts (1993).

No	RECOMMENDATION	RISK FACTOR	RELATIVE FREQ (%)	CATEGORY
1	Clarification-improvement of RFP - Contract	Incomplete - problematic -vague RFP - Contract	64	PRO
2	More IS personnel required	Insufficient IS personnel	52.5	IC
3	Clarification - improvement of project implementation plan	Incomplete - problematic - vague project implementation plan	50	PRO
4	Modification - update of technical specifications	Problematic – obsolete technical specifications	44	CO
5	Clarification - modification of project scope	Problematic - vague project scope	37.5	CO
6	Improve project team - more users participation is required	Inappropriate project team - insufficient users involvement	36	PRO
7	Interoperability with existing or under development IS infrastructure	Lack of interoperability with existing or under development IS infrastructure	34	CO
8	More emphasis on processes and organizational structures redesign - change management	Lack of processes & organizational structures redesign - lack of proper change management	32.5	CO
9	Ensure maintenance and support of the IS during its whole lifecycle	Inadequate maintenance and support of the IS after the end of the project	29	PRO
10	Exploitation of the IS that will be developed in the project by other public organizations	No exploitation of the IS that will be developed in the project by other public organizations	24	CO
11	Ensure rights on the source code of the software	Having no rights on the source code of the software	21	PRO
12	Exploit IS and data of other public organizations	No exploitation of IS and data of other public organizations	16	CO
13	More emphasis on the training of users - IS personnel	Insufficient training of users - IS personnel	15	PRO
14	Ensure the protection & exclusive use of critical - personal data entered by private enterprises	Lack of critical - personal data protection	14	PRO

No	RECOMMENDATION	RISK FACTOR	RELATIVE FREQ (%)	CATEGORY
15	Detailed technical-economic study of the networks to be developed in the project	Networks with low performance and/or very high operating cost	11	CO
16	Clarification of the general and the IS strategy of the organization, so that the project can be aligned with them	Lack of clear general and IS strategy of the organization, creating problems as to the orientation of the project	10	IC
17	Project cost reduction	Very high cost of the project	9	CO
18	More emphasis on IS security	Low emphasis on the security of the IS to be developed	7.5	CO
19	Avoid heterogeneous technologies in the project	Many heterogeneous techno-logies in the project (e.g. more than one DBMS)	6	CO
20	Ensure sufficient space for the installation of the IS	Insufficient space for the installation of the IS	6	IC
21	Prepare plans and capabilities to cope with likely future legal and/or organizational changes that will affect the IS	Legal - organizational changes are expected, that will affect the IS	5	OC

Table 1. Consolidated recommendations and risk factors

In the following paragraphs the risk factors with the highest relative frequencies are discussed and associated with the particular characteristics of the public sector, taking into account the explanations given by the members of the ITPAC during the interviews. From Table 1 we can see that there are three 'high frequency' risk factors, with relative frequencies higher than or equal to 50%. The first of them is 'Incomplete - problematic - vague Request for Proposals (RFP) and/or Contract' with relative frequency 64%. In most of the examined large projects the RFP and/or the contract needed extensive improvements and clarifications. Because of the big size and the high complexity of such IS projects it is of critical importance their RFPs and contracts to be clear and complete, describing in detail all the tasks and obligations of both parties (the contractor and the public organization However, most public organizations in Greece do not have the required capacity and experience for writing such complex, demanding and sensitive RFPs and contracts. If the RFP and/or the contract are incomplete, problematic or vague, then serious confusion and conflict might arise during the implementation of the project with negative consequences, e.g. conflicts, legal actions, delays, etc. It should also be taken into account that in Greece, and probably in many other countries, for these large IS projects there is extremely strong competition among the big companies of the ICT industry, which usually belong to big groups and corporations with high political power, good connections with the press and the other media, etc. So if the RFP and/or the contract have even a small flaw, serious problems and conflicts might arise, resulting in legal actions, interpellations in the Parliament, negative publicity in the media, big delays, etc. These characteristics of the external environment of public organizations have been highlighted by the relevant literature (e.g. Lane, 1995; Flynn, 2002; Barton, 2006; Gauld, 2007).

The second risk factor is 'Insufficient IS personnel', with relative frequency 52.5%. The ITPAC members emphasized to us that the shortage of qualified IS personnel has been a very important problem for long time since the first introduction of ICTs in the Greek Public Administration, and has been repeatedly mentioned in numerous relevant reports and official documents (Ministry to the Presidency of the Government, 1993 & 1994; Ministry of National Economy, 1994 & 2001). However, in most public organizations it has not been solved, and has caused many problems and failures in the implementation and the productive operation of many important IS projects, which were financed from various programs of the European Union and the Greek Government. This problem is associated with the difficulty of public organizations to attract highly skilled personnel, due to their salaries structures and bureaucratic mentality. The shortage of qualified IS personnel results in a reduced organizational capacity of public organizations with respect to the implementation of large IS projects, which has been repeatedly highlighted by the relevant literature (e.g. Dawes et al, 1999; OECD 2001 and 2003; Gauld, 2007).

The third risk factor 'Incomplete - problematic - vague project implementation plan', with relative frequency 50% is associated with implementation plans needing further elaboration, analysis into more detail, clarifications and modifications. According to the ITPAC members in many projects the scheduled durations of some important activities were too short, probably due to pressures from the politically appointed upper management to finish the project and show results as quickly as possible; much more time would be required, or else quite negative consequences might arise, e.g. due to incomplete users requirements analysis, limited involvement and training of the users, etc. In some very large, complex and ambitious projects, which would lead to big changes in the daily work practices of numerous public servants, a 'monolithic' implementation approach had been adopted, which would be too risky for such projects. In order to reduce this high risk, the ITPAC recommended that the implementation plans of these projects should be modified, and that modular and incremental approaches should be adopted. This risk factor is associated with the abovementioned lack of organizational capacity of public organizations for managing so large IS projects, in combination with the political environment, which is characterized by pressure for 'quick results' (Bozeman and Bretschneider, 1986; Caudle, 1991; OECD, 2001; Boyne, 2002).

Also, there are five 'medium frequency' risk factors, as we can see from Table 3, with relative frequencies between 30% and 50%. The fourth risk factor is 'Problematic - obsolete technical specifications', with relative frequency 44%. In many projects, due to the very long times required for conducting the initial feasibility studies, for the allocation of the necessary financial resources, for writing the RFP(s) and the proposed contract(s), for getting all the necessary approvals, etc., the initial technical specifications had already become obsolete at the time the project was examined by the ITPAC, because of rapid technological changes. Therefore these technical specifications should be modified and updated. The ITPAC members mentioned that in some projects the technical specifications were very narrow and restricted the competition; for this reason they recommended that they should become broader and less restrictive, or else quite negative consequences might arise, e.g. small number of good alternative solutions, higher costs, or even complaints or legal actions by some IS companies excluded due to these specifications, interpellations in the Parliament, negative publicity in the media, big delays, etc. This risk factor is associated with the quite lengthy procurement processes of public organizations and their political environment, which is often characterized by extremely strong competition among companies for winning contracts with the government.

The fifth risk factor is 'Problematic - vague project scope', with relative frequency 37.5%. In many projects the scope was vague and should be elaborated and clarified; important decisions had to be made concerning what should be included in the project and what should not. Also, from the scope of some projects were missing important activities and/or subsystems, so that a redefinition of project scope was necessary. This risk factor is also associated with the abovementioned lack of organizational capacity of public organizations for implementing so large IS projects. The sixth risk factor is 'Inappropriate project team - insufficient users involvement', with relative frequency 36%. Many project teams consisted mainly of IS personnel and only few representatives of the users; this under-representation of the users in the project team could result in insufficient understanding of users requirements, low level of users commitment to the project, etc., with quite negative consequences. Some of the ITPAC members remarked that in most of the projects having this risk factor the problems in project team composition were associated with 'silo mentalities' and intra-organizational politics and competition, which, as the relevant literature has highlighted (e.g. OECD, 2001 and 2003; Flynn, 2002; Gauld, 2007), characterize public organizations to a much higher extent than the private ones.

The seventh risk factor is 'Lack of interoperability with existing or under development IS infrastructure' with relative frequency 34%. According to ITPAC members in many projects the project teams had poor communication and coordination with the units responsible for managing the existing IS infrastructure, and also with the project teams of other IS projects being implemented in the same public organization, so proper care had not been taken for achieving interoperability among all these IS. It should be noted that there are also two similar risk factors concerning the interoperability with IS of other public organizations: 'No exploitation of the IS that will be developed in the project by other public organizations' (10^{th}, with relative frequency 24%), and 'No exploitation of IS and data of other public organizations' (12^{th}, with relative frequency 16%). These risk factors

are associated on one hand with the high complexity of the internal processes of public organizations and the strong interactions and dependencies among them, which make the interoperability among their IS necessary but at the same time difficult (Traunmuller & Wimmer, 2004; Guijarro, 2004); on the other hand they are associated with the 'silo mentalities' and intra-organizational and inter-organizational politics and competition that characterize public organizations, as mentioned above.
The eighth risk factor is 'Lack of processes and organizational structures redesign – lack of proper change management' with relative frequency 32.5%. It should be noted that this risk factor exists mainly in the largest of the examined government IS projects; the total budget of all the projects having this risk factor is 62.5% of the total budget of all the 80 examined projects. In these very large projects it was necessary to combine the development of an IS with extensive redesign of business processes and organizational structures, accompanied with a change management strategy, or else the business benefits from the IS would be very low. However, as ITPAC members noted, they did not have concrete plans for redesigning business processes and organizational structures, and for managing effectively these big changes. This risk factor is associated with the lower exposure of public organizations to markets and competition, which results in fewer incentives for change and innovation in their internal processes and structures. This trend of public organizations to avoid the redesign of their processes and structures when new IS are developed, so that finally new IS automate and reinforce existing processes and structures, has been highlighted and discussed by the relevant literature (Heintze & Bretschneider, 2000; OECD, 2001; Kraemer & King, 2006; Gauld, 2007).
It is worth remarking that all the risk factors identified in the relevant OECD Report (2001) are included in the set of risk factors we have identified in our study. However, our study, being more detailed (at the level of particular IS projects) and subsequent, has identified some additional risk factors of government IS projects (e.g. the abovementioned risk factors associated with interoperability, which have become highly important after the period covered by the OECD study).

ANALYSIS OF ORIGIN OF RISK FACTORS

Next we categorized the above 21 identified risk factors based on the framework of Willcocks and Margetts (1993) into four classes/origins: 'Process' (PRO), 'Content' (CO) 'Outer Context' (OC) and 'Inner Context' (IC) risk factors (see last column of the Table 1). For each of these four risk factors classes/origins we calculated the number of the risk factors categorized in it and the sum of their relative frequencies and the results are shown in Table 2.

ORIGIN	NUMBER OF RISK FACTORS	SUM OF REL.FREQ. OF RISK FACTORS
Outer Context (OC)	1	0.050
Inner Context (IC)	3	0.685
Content (CO)	10	2.215
Process (PRO)	7	2.290

Table 2. Number and sum of relative frequencies of risk factors for each of the classes/origins proposed by Willcocks & Margetts (1993)

We can see that the most important sources of risk are the 'Content' of the project (10 risk factors with sum of relative frequencies 2.215) and the 'Process' followed for the management and implementation of the project (7 risk factors with sum of relative frequencies 2.290). The former risk source (Content) is associated with the big size and the high complexity of such large IS projects and the corresponding public organizations, the high complexity of the interactions among them, their complex legal frameworks and the strict requirements for security and data protection. It is also associated with the need to combine the development of IS with extensive redesign of business processes and organizational structures in order to maximize benefits, which is difficult because of the limited motivation for changes and innovations that characterizes public organizations, due to their lower exposure to markets and competition. The latter risk source (Process) is associated with the

inherent difficulties and problems of managing such large and complex project (e.g. develop highly complex and demanding implementation plans, RFPs, contracts, etc., establish appropriate multi-participative project teams including representatives of the main stakeholder groups). Much lower seems to be the importance of the 'Inner Context' (3 risk factors having sum of relative frequencies equal to 0.685) and the 'Outer Context' (1 risk factor, with relative frequencies 0.050) as sources of risk.

Also from the interviews with the ITPAC members some additional inner and outer context risk factors were identified, which did not appear directly in the ITPAC Official Decisions. In particular, behind several of the identified content and process related risk factors in many projects there were some 'political factors', which were mainly associated with intra-organizational and inter-organizational politics and competition. For instance, behind risk factors 6 ('Inappropriate project team - insufficient users involvement') and 7 ('Lack of interoperability with existing or under development IS infrastructure') in many projects there were inner context factors associated with intra-organizational politics and competitions among departments and groups of the public organization developing the new IS. Also, behind factors 3 ('Incomplete - problematic - vague project implementation plan'), 10 ('No exploitation of the IS that will be developed in the project by other public organizations') and 12 ('No exploitation of IS and data of other public organizations') in many projects there were outer context factors associated with inter-organizational politics and competitions among Ministries and Ministers. Therefore these political factors, which are of a different nature than the ones identified by Gauld (2007) (external interventions through central policies, directions and 'messages' from Ministries and political leaders), can be regarded as a 'second level' risk source that influences to a considerable extent the above 'first-level' risk sources. It should be noted that such political factors exist in the private sector as well, but in the public sector they are much stronger.

Also, from the explanations given by the ITPAC members it was concluded that the importance of the inner and outer context as risk sources was in general much higher than what we had initially assessed from the analysis of the ITPAC Official Decisions. In particular, most of the identified content and process related risk factors in many projects have been generated or intensified by inner and/or outer context factors; some of them had been identified from the analysis of the ITPAC official decisions (e.g. 'Insufficient IS personnel', 'Lack of clear general and IS strategy of the organization', creating problems as to the orientation of the project), while some others were identified from the analysis of the content of our interviews with the ITPAC members (e.g. the factors associated with intra-organizational and inter-organizational politics and competition mentioned in the previous paragraph). For instance, the first risk factor 'Incomplete - problematic - vague RFP - Contract' has been generated, or at least intensified, by the lack of sufficient experienced personnel (inner context factor) and also the extremely strong competition among the big companies of the IS industry for winning government contracts (outer context factor). Similar hold for the third risk factor 'Incomplete - problematic - vague project implementation plan', which has been generated, or at least intensified, by the lack of sufficient experienced personnel (inner context factor) and the external pressure for 'quick results (outer context factor). Therefore it can be concluded that factors of the inner and the outer context of public organizations have both direct effect and indirect effect (through their effect on content and process related risk factors) on IS project failure probability.

COMPARISON WITH FINDINGS OF OTHER STUDIES

The top eleven risk factors identified in the present study were compared with i) the eleven risk factors identified in the abovementioned study of Schmidt et al (2001) to be common in the three countries it covered (Hong Kong, Finland and USA), and ii) the risk factors identified by the OECD study of risk factors of public sector IS projects, based on evidence collected from all its member states (OECD, 2001). From these comparisons we found that from the above top eleven IS projects risk factors identified in the present study:

i. five were found in the other two studies as well: 'More IS personnel required', 'Clarification – improvement of project implementation plan', 'Clarification – modification of project scope', 'Improve project team – more users participation is required' and 'More emphasis on processes and organizational structures redesign – change management; therefore these risk factors seem to be highly important in both the public and the private sector,

ii. two were found in the OECD public sector study as well: 'Clarification-improvement of RFP – Contract' and 'Modification – update of technical specifications'; these risk factors seem to be specific to the public sector,

iii. while the remaining four were not found in either of these two studies: 'Interoperability with existing or under development IS infrastructure', 'Ensure maintenance and support of the IS during its whole lifecycle', 'Exploitation of the IS that will be developed in the project by other public organizations' and 'Ensure rights on the source code of the software'; these risk factors seem to be specific to the Greece public sector, being associated with characteristics of this particular national and cultural context (e.g. the first and the third are associated with the 'silo mentality' and the problems/frictions and competitions in the inter- and intra-organizational relations, which are quite intensive in the Greek public sector; also, the second and the fourth are associated with the negative history in the relations of Greek public organizations with ICT vendors).

CONCLUSIONS, IMPLICATIONS AND FUTURE RESEARCH DIRECTIONS

In this study we investigated the risk factors of the large internal IS projects in government, based on a big sample of such projects from the Greek public sector. For this purpose we analyzed 80 Official Decisions of the Information Technology Projects Advisory Committee (ITPAC) concerning large internal IS projects of the Greek Government and conducted extensive interviews with its members. From this analysis 21 highly important risk factors were identified. The most frequent ones are 'Incomplete – problematic – vague RFP/Contract', 'Insufficient IS personnel', 'Incomplete – problematic – vague project implementation plan', 'Problematic – obsolete technical specifications' and 'Problematic – vague project scope'. The identified risk factors have been discussed and associated with the particular characteristics of the public sector, based on the details and explanations provided by the members of the ITPAC in the interviews. The above analysis shows that there are significant risk factors not only in the software development activities of the IS projects, but also in their other activities as well (e.g. in the RFPs and contracts preparation, in hardware procurement, in networks development, etc.); this justifies the 'global coverage' of the whole IS development adopted in the present study.

In order to understand better the risk generation sources and mechanisms in the large internal IS projects in government, the above 21 identified risk factors were classified as to their origin using the framework of Willcocks and Margetts (1993). It was found that the main risk origins/sources are the 'Content' of the projects and the 'Process' of managing and implementing them, while of lower importance as risk sources are the 'Inner Context' and the 'Outer Context'. However, behind several of the identified content and process related risk factors there are some 'political factors', which are mainly associated with intra-organizational and inter-organizational politics and competition, and can be regarded as a 'second level' risk source that influences the above 'first-level' risk sources. Another interesting conclusion was that factors of the inner and the outer context have not only direct effect, but also indirect effect as well on IS project failure probability, through their effect on content and process related risk factors.

The findings of this study have several implications for politicians and public sector managers:

- A critical risk factor of the large government IS projects is the lack of highly skilled IS personnel in public organizations; therefore in order to overcome this problem public organizations should develop appropriate policies, reward systems, continuous education systems, motivation schemes, etc. for attracting and retaining highly skilled IS personnel.
- Another critical risk factor is the lack of the required knowledge and organizational capacity for implementing large and ambitious IS projects in the public organizations. Taking into account that a public organization usually implements only a very small number of such large IS projects (usually not more than 1 – 2 in a decade) the acquisition of knowledge in this area is quite difficult. For this reason only a central public organization, which is competent for the monitoring, supervision and guidance of ICTs development in the whole public sector, such as the Ministry of Interior, Public Administration and Decentralization in Greece, would be appropriate for collecting knowledge from all large government IS projects and then disseminating it to the public organizations who need it.
- The 'silo mentality' and the lack of cooperation within and between public organizations very

often constitute an important risk factor of the large government IS projects. So it is necessary in such projects to create multi-participative project teams with representatives of all the groups that will be affected by the new IS (e.g. various groups of users and IS personnel); also, the members of these project teams should be appropriately motivated to cooperate, e.g. through bonuses based on the achievement of predefined objectives and in general on team performance, etc.
Further research is required in order to identify and understand better the risk factors of government IS projects in multiple national contexts, their origins, and also the risks resulting from them. Also, the relations between the identified risk factors and their impact on various project success measures should be investigated using advanced quantitative research methods (e.g. structural equation modeling. The next step could be the development and statistical validation of multi-dimensional instruments for measuring reliably government IS projects risk, consisting of multi-item constructs measuring various risk dimensions; such instruments would enable the empirical investigation of the dependence of this risk and its dimensions on various factors and of the risk patterns of various types of government IS projects. Another interesting and useful research direction is the development, pilot application and evaluation of appropriate techniques and methodologies for managing the identified risk factors and finally reducing the high failure rates of government IS projects.

REFERENCES

Barki, H., Rivard, S. & Talbot, J. (2001) *An Integrative Contingency Model of Software Project Risk Management.* Journal of Management Information Systems, 17(4), 37-69.

Boehm, B. (1991) *Software risk management: Principles and Practices*. IEEE Software, 8, 32-41.

Barton, A. D. (2006) Public sector accountability and commercial-in-confidence outsourcing contracts. *Accounting, Auditing and Accountability Journal*, 19, 256-271.

Bharadwaj, A., Keil, M. & Maering, M. (2009) Effects of information technology failures on the market value of firms. *Journal of Strategic Information Systems*, 18, 66-79.

Boyne, G. A. (2002) *Public and Private Management: What's the Difference. Journal of Management Studies*, 39, 97-122.

Bozeman, B. and Bretschneider, S. (1986) *Public Management Information Systems: Theory and Prescription*. Public Administration Review, 46, 475-487.

Buelens, M. and Van den Broeck, H. (2007) *An Analysis of Differences in Work Motivation between Public and Private Sector Organizations*. Public Administration Review, 67, 65-74.

Cabinet Office of UK (2000) *Review of Major Government IT Projects – Successful IT: Modernizing Government in Action* (http://www.ogc.gov.uk)

Caudle, S., Gorr, W. & Newcomer, K. (1991) *Key Information Systems Management Issues for the Public Sector*. MIS Quarterly, 15(2), 170-188.

Dalcher, D. & Genus, A. (2003) *Introduction: Avoiding IS/IT Implementation Failure. Technology Analysis & Strategic Management*, 15(4), 403-407

Drummond, H. (1996) The politics of risk: trials and tribulations of the Taurus project. *Journal of Information Technology*, 11, 347-357.

Fitzgerald, G. & Russo, N. L. (2005) The turnaround of the London ambulance service computer-aided system (LASCAD). *European Journal of Information Systems*, 14(3), 244-257.

Flynn, N. (2002) *Public sector management* (4th edition). Pearson Education, Harrow, UK.

Gauld, R. (2007) *Public sector information systems failures: Lessons from a New Zealand hospital organization*. Government Information Quarterly, 24, 102-114.

Goldfinch, S. (2007) *Pessimism, Computer Failure and Information Systems Development in the Public Sector*. Public Administration Review, 67, 917-929.

Goulielmos, M. (2005) *Applying the organizational failure diagnosis model to the study of information systems failure*. Disaster Prevention and Management, 14(3), 362-377.

Guijarro, L. (2004) *Analysis of the Interoperability Frameworks in e-Government Initiatives*. Proceedings of the Third International Conference EGOV 2004, Zaragoza, Spain, August 30 – September 3, 2004.

Han, W. & Huang, S. (2007) An empirical analysis of risk components and performance on software projects. *The Journal of Systems and Software*, 80, 42-50.

Heeks, R. (2003) *Success and Failure Rates of eGovernment in Developing/Transitional Countries: Overview, eGovernment for Development, Institute for Development Policy and Management*, University of Manchester, UK.

Heintze, T., & Bretschneider, S. (2000) Information Technology and restructuring in public organizations: Does adoption of information technology affect organizational structures, communications and decision making? *Journal of Public Administration Research and Theory*, 10(4), 801-830.

Jiang, J. & Klein, G. (1999) *Risks to different aspects of system success*. Information & Management, 36, 263-272.

Keil, M., Cule, P., Lyytinen, K. & Schmidt, R. (1998) *A Framework for Identifying Software Project Risks*. Communications of the ACM, 41, 76-83.

Kraemer, K., & King, J. L., (2006) Information technology and administrative reform: Will E-government be different? *International Journal of Electronic Government Research*, 2(1), 1-20.

Lai, V. & Mahapatra, R. (1997) *Exploring the research in information technology implementation*. Information & Management, 32, 187-201.

Loukis, E., Spinellis, D. & Katsigiannis, A. (2011) *Barriers to the adoption of B2B e-marketplaces by large enterprises: lessons learnt from the Hellenic Aerospace Industry*. *Information Systems Management* (accepted for publication).

Lane, J. E. (1995) *The public sector: Concepts, models and approaches*. Sage, London, UK.

Lucas, H. (1981) *Implementation: The Key to Successful Information Systems*. Columbia University Press, New York, USA.

Lyytinen, K. & Hirschheim, R. (1987*) Information systems failures – a survey and classification of the empirical literature.* In: Oxford Surveys of Information Technology, Zorkoczy, P. (ed.), 4, 257-309, Oxford University Press, Oxford.

Maylor, H. & Blackmon, K. (2005) *Researching Business and Management*. Palgrave Macmillan, New York, USA.

McFarlan, F.W. (1981) *Portfolio approach to information systems*. Harvard Business Review, 59, 142-150.

Ministry to the Presidency of the Government (1993) *Programme of Administrative Modernization 1993-1995*, Athens, Greece.

Ministry to the Presidency of the Government (1994) *Operational Programme 'Klisthenis' for the Modernization of the Greek Public Administration, European Community Support Framework II*, Athens, Greece.

Ministry of National Economy (1994) *Final Report of Integrated Mediterranean Programs on Information Technology*, Athens, Greece.

Ministry of National Economy (2001) *Operational Programme 'Information Society', European Union Support Framework III,* Athens.

Organization for Economic Co-operation & Development – OECD (2001), *'The Hidden Threat to E-Government - Avoiding large government IT failures'*, OECD Policy Brief, Paris, France.

Organization for Economic Co-operation & Development - OECD (2003) *'The e-Government Imperative'*, OECD Report, Paris, France.

Poulymenakou, A. & Holmes, A. (1996) A contingency framework for the investigation of information systems failure. *European Journal of Information Systems*, 5, pp. 34-46.

Ragin, C. (1994) *Constructing Social Research*. Pine Forge Press, California, USA.

Royal Academy of Engineering and British Computer Society (2004) *The Challenges of Complex IT Projects*, London, UK

Saarinen, T. & Vepsalainen, A. (1993) Managing the risks of information systems implementation. *European Journal of Information Systems*, 4, 283-295.

Schmidt, R., Lyytinen, K., Keil, M. & Cule, P. (2001) Identifying software project risks: an international Delphi study. *Journal of Management Information Systems*, 17, pp. 5-36.

Standish Group (1995) *The CHAOS Report*, accessed from: www.standishgroup.com.

Standish Group (2001) *Extreme chaos*, accessed from: www.standishgroup.com.

Standish Group (2004) *Third Quarter Research Report*, accessed from www.standishgroup.com.

Traunmuller, R., Wimmer, M. (2004) *e-Government: The Challenges Ahead*. Proceedings of the Third International Conference EGOV 2004, Zaragoza, Spain, August 30 – September 3, 2004.

Wallace, L., Keil, M. & Arun, R. (2004a) *How Software Project Risk Affects Project Performance: An Investigation of the Dimensions of Risk and an Exploratory Model.* Decision Sciences, 35(2), pp. 289-321.

Wallace, L., Keil, M. & Arun, R. (2004b) *Understanding software project risk: a cluster analysis*. Information & Management, 42, pp. 115-125.

Willcocks, L. & Margetts, H. (1994) Risk assessment and information systems. *European Journal of Information Systems*, 3(2), 127-138.

Wright, B. E. (2001) Public Sector Work Motivation: A Review of the Current Literature Model and a Revised Conceptual Model. *Journal of Public Administration Research and Theory*, 11(4), 559-586.

Zmud, R. (1979) *Individual differences and MIS success: a review of the empirical literature.* Management Science, 25(10), 966-979.

KEY TERMS & DEFINITIONS

Risk factor: a condition that can present serious threats to the successful completion of an IS project within budget and schedule

Outer context risk factor: a risk factor associated with outer context of the firm/organization in which the IS project is implemented, e.g. with the economy, the political environment, the government policies, the market, the competition, etc., and in the public sector with the legal framework (e.g. laws, decrees, guidelines), the funding allocations, etc.

Inner context risk factor: a risk factor associated with the interior of the firm/organization in which the IS project is implemented, e.g. with its strategy, structure, management, rewards system, human resources and industrial relations arrangements, culture, IS infrastructure and management, etc.

Content risk factor: a risk factor associated with the content of the particular IS project, e.g. with its size, technology, etc.

Process risk factor: a risk factor associated with the process of implementation of the particular IS project, e.g. with the implementation plan, the experience of the project team, the participation and training of the users, etc.