Why Do e-Government Projects Fail? Risk Factors of Large Information Systems Projects in the Greek Public Sector: An International Comparison

Euripidis Loukis, University of Aegean, Greece

Yannis Charalabidis, University of Aegean, Greece

ABSTRACT

This paper presents an empirical study of the risk factors of large governmental information systems (IS) projects. For this purpose the Official Decisions of the Greek Government Information Technology Projects Advisory Committee (ITPAC) concerning 80 large IS projects have been analyzed and interviews with its members have been conducted. From this analysis 21 risk factors have been identified, and further elaborated and associated with inherent particular characteristics of the public sector, extending existing approaches in the literature. A categorization of them with respect to origin revealed that they are associated with the management, the processes, and the content of these projects. Results show that behind the identified risk factors there are political factors, which are associated with intra-organizational and inter-organizational politics and competition, and can be regarded as 'second level' risk sources. The risk factors identified in this study are compared with the ones found by similar studies conducted in Hong Kong, Finland, and the United States, and also with the ones mentioned by OECD reports. Similarities and differences are discussed.

Keywords: *e-Government, Failure, Government, Information Systems (IS), Information Systems (IS) Projects, Public Administration, Risk Factors*

1. INTRODUCTION

Organizations of both private and public sector are making big investments for the development of various kinds of information systems (IS), in order to support and enhance their internal functions and also their communication and transaction with their external environment. However, they experience huge problems in their IS development projects: many of them fail to deliver the expected technical performance, functionality and business benefits within budget and schedule (partial failure), or even are abandoned (complete failure) (McFarlan, 1981; Boem, 1991; Standish Group, 1995, 2001, 2004; Dalcher & Genus, 2003; Gauld, 2007). For this reason there has been consider-

DOI: 10.4018/jegr.2011040104

able literature about IS projects failure, which is reviewed in the next section. However, this previous literature is focused mainly on the private sector, though government organizations experience such problems as well, of similar or even higher magnitude (Poulymenakou & Holmes, 1996; Cabinet Office, 2000; Heeks, 2003; OECD, 2001, 2003; Gauld, 2007) emphasize that in its member states governments have big problems when implementing large IT projects. These problems are regarded by OECD (2001, 2003) as 'the Hidden Threat to E-Government' and it is concluded that 'Unless governments learn to manage the risks connected with large public IT projects, these e-dreams will turn into global nightmares'. Also, previous literature is focused mainly on private sector enterprises of a few highly developed and technologically advanced countries (e.g. USA, Great Britain, etc.), and recently mainly on software development projects.

Therefore the scope of this research should be broadened. Additional research is required concerning the risk factors of government IS projects as well, in multiple cultural and socioeconomic contexts, covering the whole range of activities of the IS projects and not only software development. Also, taking into account that the limited research conducted on the risk factors of government IS projects has mainly the form of case studies, it is necessary to conduct further research on this topic based on bigger samples of projects in order to draw more generalizable conclusions.

In this direction the research objectives of the present study are:

- to investigate empirically the risk factors of the large government IS projects, based on a big sample of such projects implemented in the Greek public sector,
- to understand the main sources of risk in the large government IS projects,
- to compare with risk factors identified by similar studies conducted in other national contexts, and to identify and analyze similarities and differences.

The results of the present study are generally interesting and useful to researchers, practitioners, professional societies, educational institutions and consulting companies in the areas of public administration and information systems. It is of critical importance to reduce drastically the abovementioned high failure rates of IS projects, by systematically studying and understanding their risk factors, and by developing appropriate strategies for managing them, so that the high and ambitious IS investments made by governments of many countries (Commission of the European Communities, 2005 and 2006; United Nations, 2008) can offer the expected high levels of benefits.

This paper is organized as follows: initially in section 2 the main streams and conclusions of the previous literature on the risk factors of IS projects are briefly reviewed. Next in section 3 the research method and data are described, while in section 4 the results are presented, concerning the risk factors of large Greek Government IS projects. In section 5 these risk factors are analyzed and categorized in order to understand the basic origins of risk. In section 6 the above results are compared with the results of other similar studies conducted in other national contexts, and similarities and differences are identified and analyzed. Finally in section 7 the conclusions, implications and directions for future research are presented.

2. LITERATURE REVIEW

Understanding and reducing the unacceptably high failure rates of IS projects has been a major research topic for more than 30 years, due to the very high financial and non-financial costs of these failures. The main objectives of this research have been the identification of the 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 these risks. We have made an extensive review of this literature, and in this section in 2.1 its main three research streams are outlined (for each stream some representative studies are cited and the most important of them are discussed in more detail), followed by the main conclusions drawn from this literature review in 2.2.

2.1. Main Research Streams

The first stream investigates the risk factors of IS projects in general in various levels of detail: there are some studies at a higher level of abstraction 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 aiming to provide direct assistance to IS project managers (Zmud, 1979; Lucas, 1981; McFarlan, 1981; Lyytinen & Hirschheim, 1987; Willcocks & Margetts, 1993; Saarinen & Vepsalainen, 1993; Lai & Mahapatra, 1997; OECD, 2001, 2003; Heeks, 2003; Royal Academy of Engineering and the British Computer Society, 2004; Gauld, 2007). From this stream it is worth mentioning the work of Willcocks and Margetts (1993), who developed an interesting framework for risk analysis of IS projects, based on the conclusions of previous relevant studies. According to this framework the IS projects face four categories of risk factors as to their source. The first category of risk factors are associated with the 'Outer Context' of the organization, 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. The second category of risk factors are associated with the 'Inner Context' of the organization, e.g. with its strategy, structure, management, rewards system, human resources and industrial relations arrangements, culture, IS infrastructure and management, etc. The third category is associated with the 'Content' of the specific IS project, e.g. with its size, technology, impact, etc. Finally the fourth category of risk factors are associated with the 'Process' of the project, e.g. with the implementation plan, the experience of the project team, the participation and training of the users, etc.

With respect to public sector OECD in its relevant Policy Brief (OECD, 2001) state that governments face big problems and failures when implementing large IS projects, and identify 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. He concluded that, in addition to the risk factors found in private sector IS projects, the public sector organizations face some additional unique political and organizational risk factors, which increase failure rates. In particular, he identified critical political risk factors associated with central policies, directions and 'messages' from Ministries and political leaders (e.g. acquire 'off the self' software used by other hospitals in New Zealand), which put pressure towards selecting solutions being totally inappropriate for the particular public organization; he concludes that in the public sector there is a stronger influence of political factors as opposed to economic factors in the decision making process. Furthermore, he identified critical organizational risk factors associated with the much higher resistance to process reengineering in IS projects, the lower organizational capacity for successful IS projects implementation and the higher complexity of processes that characterizes the public sector in comparison with the private.

However, the IS practitioners' and researchers' community gradually realized that the most risky part of an IS project (i.e. the one with

Table 1. Software projects risk factors common to USA, Finland and Hong Kong

No	RISK FACTORS
1	Lack of top management commitment to the project
2	Failure to gain user commitment
3	Misunderstanding the requirements
4	Lack of adequate user involvement
5	Lack of required knowledge/skills in the project personnel
6	Lack of frozen requirements
7	Changing scope/objectives
8	Introduction of new technology
9	Failure to manage end-user expectations
10	Insufficient/inappropriate staffing
11	Conflict between user departments

the highest probability of complete or partial failure) is the software development, so a second research stream emerged focusing on the investigation of 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, 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 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 is based on three simultaneous 'ranking - type' Delphi surveys conducted in three different cultural settings: in USA, Finland and Hong Kong. It is concluded that risk factors change with time and also depend highly on the cultural, socioeconomic and organizational context. However, eleven risk factors were found, which were common to all three countries, and are shown in Table 1, in the order of their average rankings (for each of these risk factors the average of its rankings over these three countries was calculated and then used for sorting them).

Recently, after 2000, there is also a trend to investigate not only the generic risk factors that characterize IS projects in general, but also the risk factors that characterize particular types of IS projects, which are considered as highly risky, such as ERP systems projects or e-business projects, giving rise to an interesting new research stream (Sumner, 2000; Addison, 2003; Botta-Genoulaz et al., 2005; Moon, 2007).

2.2. Conclusions from Literature Review

The main conclusion from this literature review is that extensive research has been conducted for identifying and understanding the risk factors and sources of IS projects, in order to reduce the high rates of failures (complete or partial) of these projects for more than 30 years. This research has produced a useful body of knowledge, however, most of the studies that have been conducted in this area are focused on private sector enterprises, even though government organizations experience such problems and failures as well (OECD, 2001; Gauld, 2007); their conclusions cannot be directly and automatically transferred to the government organizations, due to the significant differences of public organizations in comparison with the private ones, which have been extensively analyzed and emphasized in the relevant literature (Caudle et al., 1991; Lane, 1995; Flynn, 2002) and concern their external environment, the scope and nature of their activities, their strict legal constraints, their size, internal structure and processes, etc. Furthermore, the limited research that has been conducted concerning the risk factors of government IS projects has the form of case studies; there is a lack of empirical research based on larger samples of projects which could provide more generalizable conclusions.

Also, most of the studies that have been conducted on IS projects risk factors 'have been limited by the lack of a cross-cultural perspective' (Schmidt et al., 2001), based mainly on data from USA, Great Britain and a few other highly developed and technologically advanced countries. Their conclusions reflect to some extent the cultural, business and technological context of these countries, which is quite different from the context of most other countries (e.g. developing ones); therefore further research is required on IS projects risk factors in other types of national contexts.

Another conclusion drawn from this literature review is that the most recent research on IS projects risk factors is focused mainly on software development projects; it does not investigate sufficiently 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 activities as well, e.g. request for proposals documents preparation, contracts preparation, negotiation and management activities, hardware procurement activities, networks development activities, etc. So further research is required investigating the risk factors in the whole lifecycle of an IS project.

Based on these conclusions and aiming to contribute to closing the abovementioned research gaps, this study investigates the risk factors of the large public sector IS projects in the Greek public sector. This is a very interesting national context, since Greece does not belong to the few highly developed and technologically advanced countries, has a smaller size of internal market, smaller average firm size and lower intensity of competition; also, it is characterized by lower level of ICT penetration and Internet usage in comparison with the highly developed countries, and in general limited tradition in adopting and using sophisticated technologies in both the public and the private sector.

From the numerous papers on IS projects risk factors we reviewed we selected the most relevant and appropriate ones in order to use their conclusions/findings in our study for addressing our basic research questions which have been stated in the Introduction. In particular, since one of our basic research objectives is to understand the main sources of risk in the large government IS projects, we selected to use in this study the conclusions/findings of two papers that provide frameworks for the classification of the identified risk factors as to their origin: the ones of Willcocks and Margetts (1993) and Wallace et al. (2004a). Also, since another basic research objective of this study is to compare the identified risk factors with the ones found by similar studies in other national contexts, we selected to use for this purpose the studies of Schmidt et al. (2001), OECD (2001) and Gauld (2007).

3. RESEARCH METHOD AND DATA

The research method we followed for identifying the risk factors of the large IS projects was based on the study and analysis of the 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 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 an extremely negative impact on it if not properly managed.

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 (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 (they have 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 (i.e. the Greek public sector), but do not exist in the other contexts, from which the above 'consolidated risk factors list' has been derived. Additionally, the above approach is combined with qualitative research (Ragin, 1994; Maylor & Blackmon, 2005) based on in-depth semi-structured interviews with the ITPAC members.

In particular, the research method we followed in this study included the following seven steps, which are shown in Table 2:

1. Initially, the 80 ITPAC Official Decisions between 2000 and 2005 were studied and analyzed.
2. 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. All these interviews were conducted in two or three parts of 1-2 hours duration each, tape-recorded and transcribed; finally, in each of these official decisions were attached the explanations of its recommendations provided by the ITPAC members in the above interviews.
3. 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.
4. For each of these consolidated recommendations each author working separately

Table 2. The steps of the research method followed in this study

No	RESEARCH METHOD STEPS
1	Study of ITPAC Official Decisions
2	Interviews with all members of ITPAC
3	Consolidation of recommendations
4	Determination of corresponding risk factors
5	Analysis of risk factors and association with public sector characteristics
6	Categorization of risk factors
7	Comparison with the risk factors identified in other studies

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).

5. 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.
6. The above risk factors were categorized by both authors, using the framework of Wallace et al. (2004a), and also the framework of Willcocks and Margetts (1993), in order to identify the main sources of risk in the large government IS projects.
7. Finally, these risk factors were compared by both authors in cooperation with the ones identified in the abovementioned relevant study conducted by Schmidt et al. (2001), which has based on three different cultural and socioeconomic contexts (Hong Kong, Finland and USA), and also with the ones mentioned in the relevant Policy Brief of OECD (2001).

4. RESULTS: RISK FACTORS

The consolidated recommendations and the corresponding risk factors identified in the abovementioned steps (3) and (4) are shown in Table 3 (in the second and third column respectively), in order of relative frequency (shown in the fourth column), which shows in what percentage of the 80 examined large IS projects each of them appears. Also in the last two columns of this table we can see the two categorizations of these risk factor (using the frameworks of Wallace et al. (2004a) and also Willcocks and Margetts (1993) respectively) made in the abovementioned steps (6).

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 3 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 many public organizations and their IS projects it is of critical importance their RFPs and contracts to be clear and complete, describing in detail all the tasks and obligations

Table 3. Consolidated recommendations and risk factors

No	RECOMMENDATION	RISK FACTOR	REL-FR. (%)	CAT_1 (WAL)	CAT_2 (M&W)
1	Clarification-improvement of RFP - Contract	Incomplete - problematic -vague RFP - Contract	64	PRMAN	PRO
2	More IS personnel required	Insufficient IS personnel	52.5	SOC	IC
3	Clarification - improvement of project implementation plan	Incomplete - problematic - vague project implementation plan	50	PRMAN	PRO
4	Modification - update of technical specifications	Problematic – obsolete technical specifications	44	TECHN	CO
5	Clarification - modification of project scope	Problematic - vague project scope	37.5	PRMAN	CO
6	Improve project team - more users participation is required	Inappropriate project team - insufficient users involvement	36	PRMAN	PRO
7	Interoperability with existing or under development IS infrastructure	Lack of interoperability with existing or under development IS infrastructure	34	TECHN	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	PRMAN	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	PRMAN	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	TECHN	CO
11	Ensure rights on the source code of the software	Having no rights on the source code of the software	21	PRMAN	PRO
12	Exploit IS and data of other public organizations	No exploitation of IS and data of other public organizations	16	TECHN	CO
13	More emphasis on the training of users - IS personnel	Insufficient training of users - IS personnel	15	PRMAN	PRO
14	Ensure the protection & exclusive use of critical - personal data entered by private enterprises	Lack of critical - personal data protection	14	PRMAN	PRO
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	TECHN	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	SOC	IC
17	Project cost reduction	Very high cost of the project	9	PRMAN	CO
18	More emphasis on IS security	Low emphasis on the security of the IS to be developed	7.5	TECHN	CO
19	Avoid heterogeneous technologies in the project	Many heterogeneous techno-logies in the project (e.g. more than one DBMS)	6	TECHN	CO
20	Ensure sufficient space for the installation of the IS	Insufficient space for the installation of the IS	6	PRMAN	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	SOC	OC

of both parties (the contractor and the public organization). 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 (Lane, 1995; Flynn, 2002; Gauld, 2007). However, most public organizations in Greece do not have the required capacity and experience for writing such complex, demanding and sensitive RFPs and contracts.

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 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 highlighted by the relevant literature (Dawes et al., 1999; 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’.

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 (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' (10th, with relative frequency 24%), and 'No exploitation of IS and data of other public organizations' (12th, 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

Table 4. Number and sum of relative frequencies of risk factors for each of the classes/origins proposed by Wallace et al. (2004a)

ORIGIN	NUMBER OF RISK FACTORS	SUM OF REL. FREQ. OF RISK FACTORS
Project management	11	3.140
Technical subsystem	7	1.425
Social subsystem	3	0.625

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; Kraemer & King, 2006; Gauld, 2007).

Finally, as we can see from Table 3, there are thirteen more risk factors with lower relative frequencies below 30%. We remark that the risk factor 'Insufficient training of users - IS personnel' has a low relative frequency of 15%, which shows that public organizations have realized to a large extent how important the training of users and IS personnel is for the success of their IS projects.

5. ANALYSIS OF ORIGIN OF RISK FACTORS

After analyzing and explaining each of the above 21 identified risk factors separately, we proceeded to a categorization of them in order to understand better their origin. Initially we categorized them using the framework proposed by Wallace et al. (2004) into three classes: risk factors related to the 'social subsystem' (SOC), the 'technical subsystem' (TECHN) and the 'project management' (PRMAN) (see fifth column of Table 3). In order to assess quantitatively how important each of these three risk factor classes/origins is, we calculated for each of them two indices: the number of the risk factors categorized in the particular class and the sum of their relative frequencies; the results are shown in Table 4.

From this table we can see that most of these risk factors are associated with the project management (11 risk factors in total with sum of relative frequencies 3.140), while a smaller number of them are of technical origin (7 risk factors with sum of relative frequencies 1.425) and only a few are of social origin (3 risk factors with sum of relative frequencies 0.625). This result indicates that the large size of these projects makes quite difficult several aspects of their management (such as the appropriate definition of project scope and implementation plan, the formulation of RFP(s) and contract(s), the formation of a multi-participative project team with representatives of all the stakeholder groups e.g. various groups of users and IS personnel, etc., as mentioned in the previous section); these management difficulties, in combination with the low organizational capacity of public organizations for implementing such projects, are significant sources of project risks. It should be noted that the acquisition of knowledge and experience in this area is quite difficult because a public organization usually implements only a very small number of so large IS projects (usually not more than 1 – 2 in a decade).

Also, we categorized the above 21 identified risk factors using the IS projects risk analysis framework of Willcocks & Margetts (1993) into four classes-origins: 'Process' (PRO), 'Content' (CO) 'Outer Context' (OC) and 'Inner Context' (IC) risk factors (see sixth

Table 5. Number and sum of relative frequencies of risk factors for each of the classes/origins proposed by Willcocks and Margetts (1993)

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

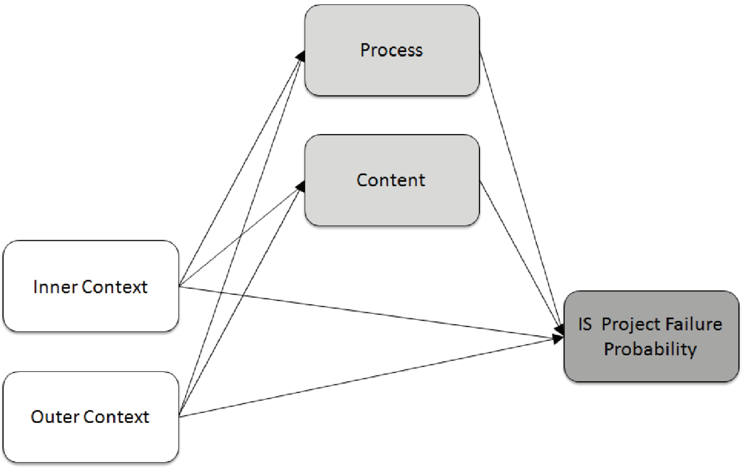
column of the Table 3). Again, for each of these four risk factors classes/origins we calculated the number of the risk factors categorized in it and the sum of their relative frequencies; the results are shown in Table 5.

From this Table we can see that the most important source 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 the public organizations and their IS projects, 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, while there is limited motivation for changes and innovations due to lower exposure of public organizations to markets and competition. The latter risk source (Process) is associated with the inherent difficulties and problems that the management of such large project poses, as mentioned above. 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

Figure 1. Direct and indirect effects of inner and outer context factors on IS project failure probability



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, as illustrated in Figure 1. This finding is in agreement with the ones of Wallace et al. (2004a) who found statistically significant relations between the basic risk sources of the software projects.

6. COMPARISON WITH RESULTS OF OTHER STUDIES

The top eleven risk factors identified in the present study were compared with the eleven risk factors identified by Schmidt et al. (2001) to be common in the relevant 'ranking - type' Delphi surveys they conducted in three countries with different cultural and socioeconomic contexts: Hong Kong, Finland and USA. It should be noted this study is not focused on the public sector of these countries, and is based on the overall experience that the participants in the Delphi surveys had from both the private and the public sector. For each of the top eleven

Table 6. Comparison between the risk factors identified in the present study and the risk factors identified by Schmidt et al. (2001) and by OECD (2001)

No	Risk factors of the present study	Similar risk factors identified bySchmidt et al (2001)	Similar risk factors identified byOECD (2001)
1	Incomplete - problematic - vague RFP - Contract	N/A	Weaknesses in managing relationships with external vendors
2	Insufficient IS personnel	Insufficient/inappropriate staffing (10) Lack of required knowledge/skills in the project personnel (5)	Lack of specialized and knowledgeable human resources
3	Incomplete - problematic - vague project implementation plan	No Planning or inadequate planning (Finland - 10)	N/A
4	Problematic – obsolete technical specifications	N/A	Use of emerging and still immature technologies
5	Problematic - vague project scope	Unclear/misunderstood cope/ objectives (USA - 9)	N/A
6	Inappropriate project team - insufficient users involvement	Lack of required knowledge/skills in the project personnel (5) Insufficient/inappropriate staffing (10) Lack of adequate user involvement (4)	Limited involvement of end-users and inappropriate governance structures
7	Lack of interoperability with existing or under development IS infrastucture	N/A	N/A
8	Lack of processes & organizational structures redesign - lack of proper change management	Not managing change properly (USA - 3, Finland - 4)	Focus on business process change
9	Inadequate maintenance and support of the IS after the end of the project	N/A	N/A
10	No exploitation of the IS that will be developed in the project by other public organizations	N/A	N/A
11	Having no rights on the source code of the software	N/A	N/A

risk factors of the present study, we examined whether it can be matched with any of the eleven common risk factors identified in the above study. The results are shown in the second column of Table 6.

We can see that two out of the top eleven risk factors ('Insufficient IS personnel' and 'Inappropriate project team-insufficient users involvement') can be matched with one or more of the above eleven common risk factors identified by Schmidt et al. (2001). Also three more of the risk factors ('Incomplete - problematic - vague project implementation plan', 'Problematic - vague project scope', 'Lack of processes & organizational structures redesign - lack of proper change management') of the present study can be matched (at least to some extent) with one or more of the risk factors identified by Schmidt et al. (2001) only in one or two of the above three countries. The remaining six risk factors of the present study cannot be matched with any of the risk factors identified by Schmidt et al. (2001).

Therefore between the risk factors identified in the present study and the ones identified by Schmidt et al. (2001) there some similarities, but also there are significant differences as well. In particular the first of the risk factors identified in the present study ('Incomplete - problematic - vague RFP - Contract') does not appear in any of the lists of Schmidt et al. (2001). This difference is associated with the big size and the high complexity of the large government IS projects, and also with the complex legal frameworks and legalistic mentality of public organizations (which in Greece is quite strong). It is also associated with the political environment of public organizations, which is characterized by extremely strong competition among big companies of the ICTs industry (most of them having high political power, good connections with the press and the other media, etc.) for winning contracts with the government, high level of public scrutiny of government contracts and projects, etc.

Also the fourth of the risk factors identified in the present study ('Problematic - obsolete technical specifications') does not appear in any of the lists of Schmidt et al. (2001). This difference is associated with the highly complicated and long procurement processes of the public sector, which make the initial technical specifications obsolete by the time the project is examined by the ITPAC. It also reflects the obligation of public organizations to avoid very narrow technical specifications that result in the exclusion of most ICT vendors and restrict the competition. Furthermore, two of the most important risk factors identified in the present study, which both concern interoperability with other IS in the same public organization or in other public organizations ('Lack of interoperability with existing or under development IS infrastructure' and 'No exploitation of the IS that will be developed in the project by other public organizations') do not appear in any of the lists of Schmidt et al. (2001). This difference is associated with the high complexity of both the internal processes of public organizations and the interactions and interdependencies among them, and also with the 'silos' structure and mentality that characterize public organizations.

The risk factors identified in the present study were also compared with the ones mentioned in the relevant OECD Policy Brief (OECD, 2001). This Policy Brief is dealing with the failures and the risk factors of public sector IS projects and is based on OECD's long experience. Again, for each of the top eleven risk factors of the present study, we examined whether it can be matched with any of risk factors mentioned by OECD; the results are shown in the third column of Table 6. We can see that five out of the top eleven risk factors of the present study can be matched (at least to some extent) with one or more of the risk factors mentioned by OECD. One of them is the first of the risk factors identified in the present study with the highest relative frequency concerning 'Incomplete - problematic - vague RFP – Contract', which can be matched to some extent with the risk factor concerning 'weaknesses in managing relationships with external vendors' mentioned by the OECD; this confirms that the complete and detailed definition of the relationships with external IT vendors in both the RFPs and the contracts is quite important for the success of large government IS projects, much more than in the private sector. Also the risk factor 'Problematic – obsolete technical specifications' can be matched to some extent with the 'Use of emerging and still immature technologies' risk factor mentioned by the OECD; this confirms the importance of appropriate technical specifications for the large government IS projects. Finally, the risk factors 'Insufficient IS personnel', 'Inappropriate project team - insufficient users involvement' and 'Lack of processes & organizational structures redesign - lack of proper change management' can also be matched by similar risk factors from the above OECD Policy Brief; taking into account that the above risk factors had also been matched with one or more of the ones of the study of Schmidt et al. (2001) indicates that these risk factors are highly important for the success of IS projects both in the public and the private sector.

Summarizing, based on the above comparisons we can divide the above top eleven IS projects risk factors identified in the present study into three groups:

- Risk factors which are highly important in both the public and the private sector (factors 2, 3, 5, 6 and 8)
- Risk factors which are highly important only in the public sector (factors 1 and 4)
- Risk factors which are specific to the context of the public sector of Greece and possibly other countries with a similar level of economic and technological development (factors 7, 9, 10 and 11).

7. CONCLUSIONS, IMPLICATIONS AND FUTURE RESEARCH DIRECTIONS

7.1. Summary of Conclusions

In this study we investigated the risk factors of the large government IS projects, based on a big sample of such projects from the Greek public sector. We analyzed 80 Official Decisions of the Information Technology Projects Advisory Committee (ITPAC) concerning large 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 frequently appearing 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 associated with the particular characteristics of the public sector, based on the details and explanations given 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 the other activities as well (e.g. in the RFPs and contracts preparation, in hardware procurement, in networks development, etc.), which have been neglected by previous literature.

In order to understand better the risk generation sources and mechanisms in the large government IS projects, the above 21 identified risk factors were classified as to their origin using the frameworks of Wallace et al. (2004a) and Willcocks and Margetts (1993). It was found that most of these risk factors are associated with the project management, while a smaller number of them are of technical origin and only a few are of social origin. Their 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 (through their effect on content and process related risk factors) on IS project failure probability. Finally, the risk factors identified in the present study were compared with the ones identified in a similar study conducted by Schmidt et al. (2001) in Hong Kong, Finland and USA, and also with the ones mentioned in the relevant Policy Brief of OECD (2001). From this comparison it was concluded that some of the identified IS projects risk factors are specific to the public sector, while some others appear in the private sector as well, as discussed at the end of the previous section.

7.2. Implications for Politicians and Managers

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, motives, 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 use of consultants' services should be regarded only as a secondary and complementary mechanism for the acquisition of knowledge in this area, taking into account that the over-reliance on consultants in combination with low organizational capacity for monitoring their services and evaluating their suggestions can have quite negative impacts (Gauld, 2007).
- 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.

7.3. Future Research Directions

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) (Kline, 2005); the model of Figure 1 could be used as basis for future research in this direction. 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

Addison, T. (2003). E-commerce project development risks: Evidence from a Delphi survey. *International Journal of Information Management*, *23*, 25–40. doi:10.1016/S0268-4012(02)00066-X

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. doi:10.1109/52.62930

Botta-Genoulaz, V., Millet, P. A., & Grabot, B. (2005). A survey of the recent literature on ERP systems. *Computers in Industry*, *56*, 510–522. doi:10.1016/j.compind.2005.02.004

Cabinet Office of UK. (2000). *Review of major government IT projects – successful IT: Modernizing government in action.* Retrieved from http://www.ogc.gov.uk

Caudle, S., Gorr, W., & Newcomer, K. (1991). Key information systems management issues for the public sector. *Management Information Systems Quarterly*, *15*(2), 170–188. doi:10.2307/249378

Commission of the European Communities. (2005). *i2010 – a European information society for growth and employment*. Retrieved from http://www.eluxembourg.public.lu/eLuxembourg/i2010.pdf

Commission of the European Communities. (2006). *i2010-eGovernment Action Plan: accelerating egovernment in Europe for the benefit of all.* Retrieved from http://ec.europa.eu/information_society/activities/egovernment/docs/action_plan/comm_pdf_com_2006_0173_f_en_acte.pdf

Dalcher, D., & Genus, A. (2003). Avoiding IS/IT implementation failure. *Technology Analysis and Strategic Management*, *15*(4), 403–407. doi:10.1080/095373203000136006

Dawes, S., Bloniarz, P., Connelly, D., Kelly, K., & Pardo, T. (1999). Four realities of IT innovation in government. *Public Management*, *28*(1), 1–5.

Flynn, N. (2002). *Public sector management* (4th ed.). London, UK: Pearson Education.

Gauld, R. (2007). Public sector information systems failures: Lessons from a New Zealand hospital organization. *Government Information Quarterly*, *24*, 102–114. doi:10.1016/j.giq.2006.02.010

Guijarro, L. (2004, August 30-September 3). Analysis of the interoperability frameworks in e-government initiatives. In *Proceedings of the Third International Conference EGOV,* Zaragoza, Spain.

Han, W., & Huang, S. (2007). An empirical analysis of risk components and performance on software projects. *Journal of Systems and Software*, *80*, 42–50. doi:10.1016/j.jss.2006.04.030

Heeks, R. (2003). *Success and failure rates of egovernment in developing/transitional countries: Overview.* Retrieved from http://www.egov4dev.org/success/sfrates.shtml

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 access of system success. *Information & Management*, *36*, 263–272. doi:10.1016/S0378-7206(99)00024-5

Keil, M., Cule, P., Lyytinen, K., & Schmidt, R. (1998). A framework for identifying software project risks. *Communications of the ACM*, *41*, 76–83. doi:10.1145/287831.287843

Kline, R. B. (2005). *Principles and practice of structural equation modeling*. New York, NY: Guilford Press.

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. doi:10.4018/jegr.2006010101

Lai, V., & Mahapatra, R. (1997). Exploring the research in information technology implementation. *Information & Management*, *32*, 187–201. doi:10.1016/S0378-7206(97)00022-0

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

Lucas, H. (1981). *Implementation: The key to successful information systems*. New York, NY: Columbia University Press.

Lyytinen, K., & Hirschheim, R. (1987). Information systems failures – a survey and classification of the empirical literature. In Zorkoczy, P. (Ed.), *Oxford surveys of information technology* (*Vol. 4*, pp. 257–309). Oxford, UK: Oxford University Press.

Maylor, H., & Blackmon, K. (2005). *Researching business and management*. New York, NY: Macmillan.

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

Ministry of National Economy. (1994). *Final report of integrated Mediterranean programs on information technology.*

Ministry of National Economy. (2001). *Operational programme 'information society': European union support framework III.*

Ministry to the Presidency of the Government. (1993). *Programme of administrative modernization 1993-1995.*

Ministry to the Presidency of the Government. (1994). *Operational programme 'Klisthenis' for the modernization of the Greek public administration: European community support framework II.*

Moon, Y. B. (2007). Enterprise resource planning: A review of the literature. *International Journal of Management and Enterprise Development*, *4*(3), 235–264. doi:10.1504/IJMED.2007.012679

Organization for Economic Cooperation & Development (OECD). (2001). *The hidden threat to e-government - avoiding large government it failures*. Paris, France: OECD.

Organization for Economic Cooperation & Development (OECD). (2003). *The e-government imperative*. Paris, France: OECD.

Poulymenakou, A., & Holmes, A. (1996). A contingency framework for the investigation of information systems failure. *European Journal of Information Systems*, *5*, 34–46. doi:10.1057/ejis.1996.10

Ragin, C. (1994). *Constructing social research*. Thousand Oaks, CA: Sage.

Royal Academy of Engineering and British Computer Society. (2004). *The challenges of complex IT projects*. London, UK: The Royal Academy of Engineering.

Saarinen, T., & Vepsalainen, A. (1993). Managing the risks of information systems implementation. *European Journal of Information Systems*, *4*, 283–295. doi:10.1057/ejis.1993.39

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

Standish Group. (1995). *The CHAOS report.* Retrieved from http://www.standishgroup.com

Standish Group. (2001). *Extreme chaos*. Retrieved from http://www.standishgroup.com

Standish Group. (2004). *Third quarter research report.* Retrieved from http://www.standishgroup.com

Sumner, M. (2000). Risk factors in enterprise-wide ERP projects. *Journal of Information Technology*, *15*, 317–327. doi:10.1080/02683960010009079

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

United Nations. (2008). *UN e-Government survey 2008: From e-Government to connected governance*. New York, NY: United Nations.

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), 289–321. doi:10.1111/j.00117315.2004.02059.x

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

Willcocks, L., & Margetts, H. (1994). Risk assessment and information systems. *European Journal of Information Systems*, *3*(2), 127–138. doi:10.1057/ejis.1994.13

Zmud, R. (1979). Individual differences and MIS success: A review of the empirical literature. *Management Science*, *25*(10), 966–979. doi:10.1287/mnsc.25.10.966