FRAMES – A Risk Assessment Framework for e-Services

Adrianos Evangelidis
International Teledemocracy Centre, Napier University, Edinburgh, Scotland, UK
a.evangelidis@napier.ac.uk

Abstract: e-Government projects are expected to increase efficiency and quality of government services, whilst decreasing the costs. Unfortunately though, together with its perceived positive potential, e-Government also entails risks. It is expected that the employment of proper risk assessment methods in the management of such projects will reduce the threats imposed by the various risks that surround these projects. This paper discusses about risk in e-Government and provides a high-level e-Government risk factor classification. Furthermore, this article proposes a novel risk assessment framework for e-Services in the public administration.

Keywords: e-Government, e-Service, Risk, Risk Assessment, Frameworks

1. Introduction

The recent trend for public administrations worldwide is to implement e-Government. This originates from the expected outcomes that the introduction of Information and Communication Technologies (ICTs) may bring to the public sector. The profits of the informatisation of the public sector may be increased efficiency and effectiveness, decreased costs and better quality of services. Therefore, governments are investing heavily and setting tight deadlines on e-Government projects in order to exploit the expected benefits.

In order to achieve such outcomes, e-Government projects have to be successfully designed and deployed. These are non-trivial tasks. Recent reports in the UK (Arnott 2003) show that the cost of cancelled or over-budget government IT projects has topped £1.5billion in the last six years. For example, just a single cancelled e-Government project on smartcards resulted in a loss of £698million to the British government. Similar situations may be avoided or at least better handled through appropriate risk assessment strategies. Such strategies may be able to enhance decision-making by turning threats into opportunities for success and provide better project management through the enabling of contingency plans.

Within that context, a current research programme investigates the risks associated with e-Government projects (*see also* Akomode et al. 2002; Evangelidis et al. 2002; Evangelidis and Macintosh 2003) in order to investigate the effect of a qualitative multi-perspective risk assessment framework for e-Government services (or government e-Services). e-Services for government are simply the 'online' services (Hoogwoot 2002 p.33) that are provided by the public administration within an e-Government environment. As Gordon (2002) explains government services are delivered with various levels of interaction. Three levels are usually identified: information, communication, and transactions. Information services deliver government information via static web pages and pages generated from databases to citizens, tourists, businesses, associations, public administration, and other government users. Communication services use groupware technology such as e-mail, discussion forums and chat to facilitate dialogue, participation and feedback in planning and policy-making procedures. Therefore, according to Gordon (2002, p.12) transaction services use online forms, workflow and payment systems to allow citizens and business partners to take care of their business with government online. Typical applications of transaction services for citizens include applying for social benefits, registering automobiles, filing changes of address or applying for building permits. For businesses, perhaps the application of greatest current interest is the online procurement of government contracts.

Such a framework is expected to be used by managers, researchers and members of e-Government projects. To explore this research topic an analytical framework is required. This paper describes the novel

framework FRAMES, which stands for Framework for Risk Assessment and Modelling in E-Government Services. This framework aims at the provision of a methodology for efficient risk assessment in e-Government transaction services and is expected to be evaluated within collaborating establishments, at both local and national government levels.

2. Risk in e-Government

e-Government projects are inherently complex, mostly sharing similar risks with their eBusiness counterpart projects. This is logical as both concepts (e-Government and e-Business/e-Commerce) share some striking similarities. Such common characteristics may be the similar infrastructures, the transformation of business, the collapse of organisational boundaries, as well as the common goals, just to name a few (for more on such comparison read Gisler 2000; Dridi 2001; Greunz, 2001; Traunmüller 2000). Hence, some scholars define e-Government in relation to e-Business or eCommerce. For example, Howard (2001) states that "*e-Government is the application of the tools and techniques of eCommerce to the work of government*". Similarly, Schubert (2001) portrays electronic business as a subset of electronic government. Within that context, there are also common risks that may be found in both areas.

Some typical risks that may be experienced in both domains can be listed as follows: a) uncertain timescale prediction, b) increased delays and costs, c) misinformed decisions, d) reliance on technology, e) security risks and f) risks related to the unpredictable nature of the ICTs. Of course such enlisting is far from exhaustive, but it gives a flavour of some common risks shared in both the e-Government and e-Business fields (for e-Business related risks read Labuschagne 2000; Frynas 2002; Adam 1996 and for e-Government related risks read Akomode 2002; Evangelidis 2002).

Implementing e-Government as a major development can be a daunting task, since it can involve many factors of risk that could threaten the success of the project. Adequate risk assessment procedures may help in avoiding major pitfalls, though sometimes failures cannot always be predicted precisely. Since electronic government projects have a broad scope, risks can be found in many diverse areas. To name a few, such areas may be related to the technological foundations of the e-Government phenomenon, may be involved to the social aspect of electronic government, there can even be some political areas where risks might arise. Therefore, risk assessment in e-Government, if explored holistically, should span on a very broad and multidisciplinary environment in order to have a reasonably adequate positive effect.

3. e-Government Risk Areas - STEPS

To support such a framework the need arises for a categorisation of the various risk factors that surround e-Government projects. This part of the paper shall introduce the main risk factors areas that will be considered for extracting risk elements to be used in the risk assessment process. It has to be stressed here this discussion will not delve any deeper as it is out of the scope of this paper.

Experience from the electronic commerce/business domain and the relevant literature show that some have attempted to classify risks in all sorts of high-level categories according to the nature of the risks. To name a few, Tchankova (2002) proposed seven different classes of risks, namely: i) physical, ii) social, iii) political, iv) operational, v) economic, vi) legal, and vii) cognitive environment. Additionally, Liebermann (2002) distinguished five different areas of risk in the eCommerce field, which are the: i) financial, ii) physical, iii) psychological, iv) social, and v) technological. Furthermore, in the 'Integrated Risk Management Framework' (Treasury Board of Canada Secretariat 2001 p. 9) the following main classification of potential risks influencing an organisation are identified: i) political, ii) economic, iii) social, and iv) technological.

In that fashion and for the purposes of this research programme this paper proposes the following high level classification of risk factors that surround e-Government projects:

a) Societal – referring to the risks that usually affect the way people live and interact in the society
b) Technical – such risks arise from the way information and communication technologies are used in order to serve the purposes a particular project is meant for
c) Economical – where financial related risks are indicated
d) Political – here risks that erupt from government policies/decisions are discussed. It has to be stressed here that under the 'political' risk umbrella the legal-related risks are also included.
e) Security – since security has a major importance in e-Government projects it has to have a risk class on each own.

This paper names this classification STEPS (after the first letter of each class) and it is believed that such approach can be useful mainly for two reasons: i) to help (by giving a holistic view) the risk assessor create his/her risk assessment plan more efficiently, and ii) so as to put an order to the numerous high level risks involved, which will help in better exploiting such risk identification.

4. e-Government frameworks

To structurally develop FRAMES in its current form, various e-Government frameworks have been examined. The reason for doing so was the possible discovery of existing frameworks or models that look at the phenomenon in a holistic manner. Therefore, they could provide the foundations for the design of a risk assessment framework or even better, a suitable one could be re-used as is by 'attaching' risk assessment methods on top of it. These frameworks/models could be distinguished into two types: i) strategic, since they define the strategies that have to be followed to better realise e-Government, and ii) operational, since they describe various architectures of e-Government systems.

Four strategic designs have been found. One of them, the 'Value Chain Model' (Wassenaar 2000) demonstrates the way e-Government may add value to the public sector. As such, it explores the e-Government concept from a business perspective and it is all about helping public administrators to better understand and realise the potential of exploiting the ICTs in the public sector. A second one attempts to set the various viewpoints from which e-Government systems may be viewed (for more details read Lenk 2000; Papantoniou 2001). The ultimate aim of this framework is to shape the future of e-Government by setting some guidelines based on the following four perspectives: a) addressee, b) process, c) co-operation, and d) knowledge. A third strategic design for e-Government is the 'three dimensional viewing of e-Government' (Gisler 2000; Papantoniou 2001) of any e-Government system. A fourth strategic design for e-Government that has been identified from the literature review is the 'Growth Model' (Layne 2001) which describes four (growth) stages that lead towards fully functional e-Government.

Likewise, the literature survey divulged two operational models for e-Government. The first one simply discusses about two different types of e-Government architectures coupled with their advantages and disadvantages (Laprø 2000). These two architectures are called the 'integration' and 'fragmentation' model and basically discuss about the 'positioning' of the back office and the front office. Finally, the second operational model provides another design principle for e-Government implementations. The 'general model for e-Government initiatives' (Dridi 2001) describes two perspectives; the external and internal ones that are equally important for developing e-Government projects.

Such frameworks, despite the fact that they can provide holistic views of the e-Government concept from various angles have been proven unsatisfactorily for the purposes of this research. The Value Chain Model is a very useful business oriented framework, but unfortunately it is deemed that is not applications specific, as needed for this research project. Then, two other strategic frameworks, the 'three-dimensional' and the 'viewpoints' ones, do pose very good designs in order to assist in setting policies and long term goals for e-Government implementations, but they seem to be rather too high-levelled for risk assessment to be efficient. In regards to the fourth strategic framework, the 'Growth Model' it has to be stressed that it is a very useful template in order to examine how e-

Government projects progress. Unfortunately though, it does not describe any structural elements of such projects, thus it may not be very useful as the basis of a risk assessment framework. Furthermore, and after examining the remaining two operational frameworks/models, the following may be concluded. In regards to the 'integration/fragmentation' model it may be said that it is a nicely structured architectural model for e-Government services that is focused on the back and front office and how these are positioned, but unfortunately it does not go any deeper. For instance, what happens in the back office? As such, it is two vague for the purpose of this research programme's aims. And finally, the 'general model for e-Government initiatives' poses a very all-round high-level framework that may provide guidelines for effective e-Government implementation, but unfortunately it is not very descriptive at a more lower, more 'apt', level so that efficient risk assessment methods could be employed.

5. FRAMES – A Framework for Risk Assessment and Modelling in e-Government Services

As explained in the introduction, the Framework for Risk Assessment & Modelling in e-Government Services aims at the provision of a methodology for efficient qualitative risk assessment in e-Government services.

The main aims of FRAMES can be summarised in the following three statements:

- To provide a holistic view of an e-Government transaction service project
- To enable the decision maker in assessing the risks involved in the development of the electronic transaction service.
- To enhance decision-making at the feasibility stage of the project development.

This paper accepts that any electronic government transaction service can be seen as a socio-technical system (or STS). Socio-technical systems (Kavan 1999) usually consist of two subsystems; the social subsystem and the technical subsystem, which are interdependent (*see Figure 1*). The social subsystem contains two components: i) the structure (or roles), i.e. Communications, authority, workflow systems, and ii) the people that have various such as attitudes, skills, and values. On the other hand, the technical subsystem contains two components as well: i) the technology that is required for the system, and ii) the task(s) needed to achieve the goals of the system.

Within that context FRAMES provides a way of implementing risk assessment in e-Services. As such, any e-Government transaction service project is seen (*Figure 2*) as an STS that comprises of three main socio-technical subsystems that interconnect four main modules of the transaction service project. These four main modules are: i) the customers, ii) the e-Service, iii) the organisational level, and iv) the intra-organisational service.

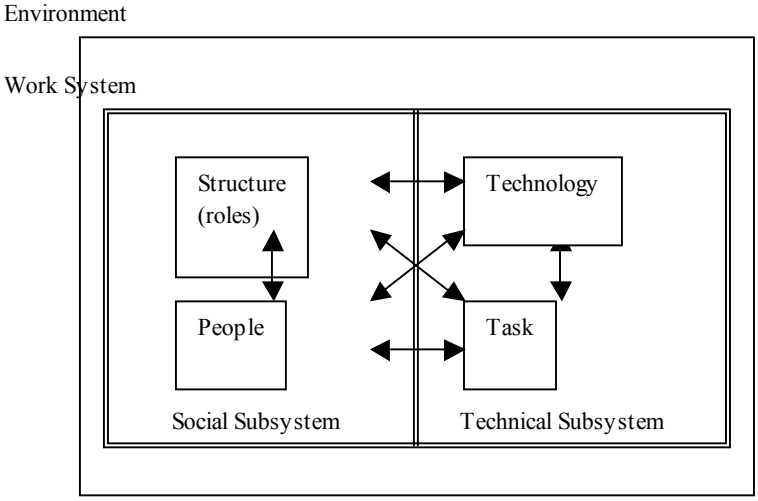

Figure 1: Socio-Technical System (adapted from Bostrom 1980; cited in Kavan 1999 p.297)

The 'customers' module mainly refers to the customers/users of the transaction service. These users can be citizens or businesses (and in some cases other governments) that interact with the front end of the system. Such interaction is understood to be in the form of using the system and/or providing feedback to the system. The second main module of FRAMES is the e-Service itself and it is divided into two main parts; a) the front end that is the main application/function that the customer is interacting with, and b) the back end that denotes the point where the eService interacts with the 'parent' organisation, namely the public authority, which is responsible for the service, as well as other organisations that contribute, share information, interact with the eService. The third main module within FRAMES is the organisational level and it basically refers to the public authority that is responsible for the development of the electronic government transaction service. Within that level, the main actors / functions that support / develop the electronic transaction service can be found. Finally, the fourth main module within FRAMES is the intra-organisational level that usually entails, other than the public authority, organisations (governmental or non-governmental) that are needed to support / develop the e-Service.

As it was mentioned above, within FRAMES there are three major socio-technical subsystems that are formed between the modules of the system. One such subsystem is formed by the connecting relationship of customers and the front end of the eService. A second socio-technical subsystem is formed by the connecting relationship between the organisational level and the back end of the e-Service module. And finally, a third such subsystem is formed between the back end of the e-Service module and the intra-organisational level. Such subsystems are of crucial importance and are needed within FRAMES in order to better 'customise' the risk assessment process within any e-Government transaction service project. As mentioned earlier, each of these subsystems contains people that have different roles and utilize technology to achieve certain tasks that will work towards the system's goals. FRAMES understands that there are various typical high level risks within these particular areas (and this is were STEPS is going to be exploited).

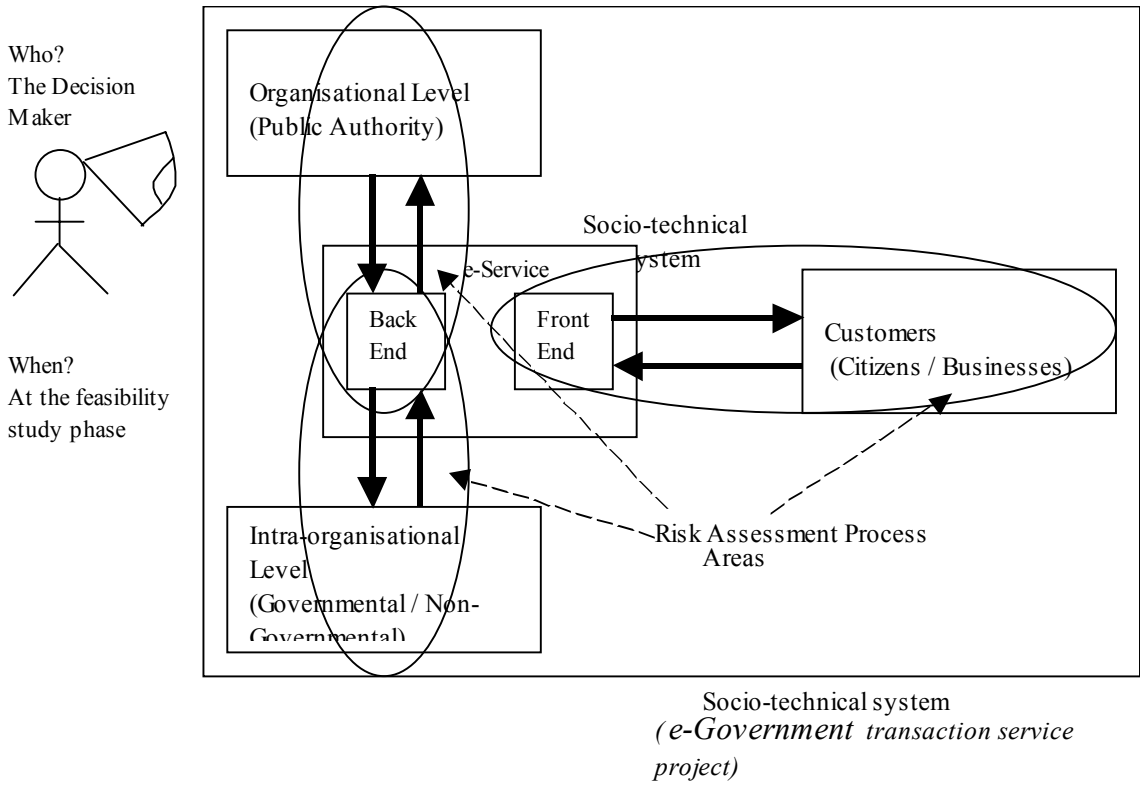

Figure 2: FRAMES

FRAMES adopts from the BS-6079-3 Standard the risk assessment sub-process. Therefore, the risk assessment process within FRAMES will consist of the following stages (*see figure 3 below*): i) context establishment, ii) risk identification, iii) risk analysis, and iv) risk evaluation.

Context Establishment – The first stage of FRAMES is responsible for establishing the broad context within which risk assessment will be done. This stage mainly (but not limited to) includes knowledge acquisition, which will eventually set the measures of the various risks' impact. The knowledge acquisition stage defines the long term (strategic) goals of the system/organisation, as well as the medium term (organisational) goals and the short term (management) goals. Then the risk assessor has to define the threats to these goals. Furthermore, another part of the 'context establishment' stage is to develop various criteria, such as to decide on the key actors/stakeholders. The final phase of this stage is to decide on the structure, which will tackle the issue of choosing what sort of qualitative risk assessment approach /approaches is more suitable, as well as the initial presentation of the risk assessment area to the stakeholders.

Risk Identification – Here lies the process of identifying the risks, as well as how, what or why incidents may occur. To achieve risk identification various methods can be used each of them having their own advantages and disadvantages. FRAMES will employ risk identification techniques that enable qualitative risk assessment. Some of them may be the following: i) semi-structured interviews, ii) brainstorming, iii) Nominal Group Technique, iv) Delphi method, and v) checklists. Of course other suitable qualitative techniques can be used in FRAMES.

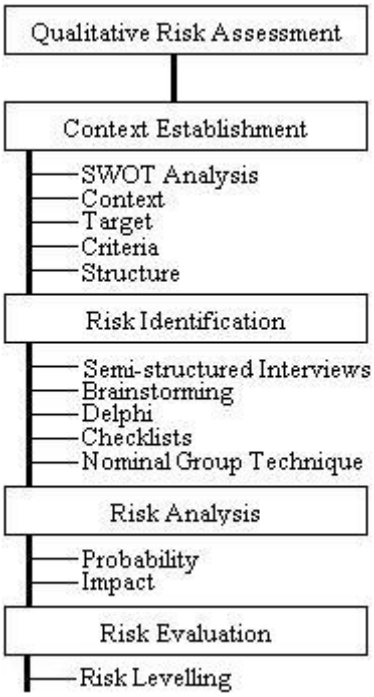

Figure 3: Risk assessment stages

Risk Analysis – It is a stage, where an estimation of both the probability of the occurrence of a risk and the magnitude of the consequences of the risk happens.

Risk Evaluation – During this process the consequences of the risks are levelled after their impact/magnitude.

6. Benefits and application

Certain benefits are expected to be reaped from the introduction of appropriate risk assessment strategies in e-Government projects. First of all, the obvious may happen that is an overall reduction in risk exposure. Such strategies should also aid in the improvement of decision-making,

since there shall exist a comprehensive and structured understanding of the activities, opportunities and threats involved in the project. Furthermore, following the guidelines of a risk assessment framework, e-Government project managers will achieve to enable future activities happening in a consistent and controlled manner. The benefits of systematic e-Government risk assessment are also expected to improve the control of project costs, quality and time, factors that are extremely important, since they are the precursors for the balancing of 'side-effects' such as citizens' satisfaction, public authorities' image and others. e-Government is surely a quite modern concept and therefore its evolving terminology is still not 'standardized', meaning that e-Government managers might be using different terms whilst talking about the same subject, which results to undesirable effects. Fortunately, with the introduction of a holistic risk assessment framework people interested in e-Government will now use a common language, thus can better communicate about various e-Government issues.

More specifically, it is expected that this risk assessment framework will provide numerous of positive outcomes to the users. First of all, FRAMES should act as a template which will show the main sources of risk that surround e-Government implementations. Additionally, it can be used as a template for risk assessment in e-Government projects that can be fully customised for the particular needs of individual projects. Furthermore, FRAMES will also assist in providing guidance on how to do efficient qualitative risk assessment in any e-Government project. Additionally, this framework is designed to provide electronic government users an integrated systems view of all major issues involved in the identification and analysis of high level risks. The 'whole picture' provided by FRAMES should enable e-Government managers to efficiently understand and use the various stages of the risk assessment process within electronic government implementations. It is also expected that this framework for qualitative risk assessment in e-Government should enhance awareness on the various threats and opportunities that are normally associated with e-Government projects as well as provide the opportunity to e-Government managers to calculate the significance of the various risks and aid them in a better decision-making process. For example, such awareness can be useful during contract negotiations or for the development of alternative contingency plans.

As it was originally thought and subsequently supported by the opinion of three experts in e-Government at a recent field research (for more on that read Evangelidis 2004) there can be at least two main areas of application that FRAMES is primarily aiming at. The 'qualification' stage may be seen as the first practical use of FRAMES. That stage is where many ideas for potential government eServices are proposed and FRAMES can be used there in order to avoid waste and to choose the best candidate for a potential e-Government service, thus saving resources and effort for the developing organisation. Furthermore, a second potential example of where such a framework may be implemented in practice is the planning of the actual e-Government services. It is apparent that by having a 'knowledge base' of potential risks and using it as a template, through FRAMES, planning for eServices could become so much easier.

7. Conclusions

The Electronic Government phenomenon is gaining momentum at a quick pace. Worldwide, public administrations seem to invest heavily on that trend. Unfortunately though, together with its expected dynamic potential this concept surely entails some risks, which can become threats (if not taken care of); or exploitable opportunities, if systematic risk assessment methods are put in place. This paper introduced the reader to the e-Government risk and provided a high-level risk factors classification termed STEPS. Furthermore, this article introduced and described a novel qualitative multi-perspective risk assessment framework for e-Services in the public administration, which is called FRAMES. Potentially, such risk assessment framework may find applicability in areas like planning or qualification for eServices in the public sector.

References

Adam, N., R., Yesha, Y. 'Electronic Commerce: Current Research Issues and Applications*'* Springer, (1996)

Akomode, J, Taleb-Bendiab, A, Evangelidis, A, Taylor, M 'UML Approach to Risk Assessment Modelling for e-Government' In *Proceedings of the 2nd European Conference on E-Government* St. Catherine's College Oxford UK (2002) pp 395-402.

Arnott, S '£1.5bn Squandered on Government IT' *Computing*, (March 13 2003) p.1.

Bostrom, R 'A Socio-Technical Perspective on MIS Implementation' *Paper presented at ORSA/TIMS* Colorado Springs USA (1980).

Dridi, F., Pernul, G., Unger, V. 'Security for the Electronic Government' *Proceedings of the 1st European Conference on e-Government*, Trinity College Dublin, Ireland, (2001) pp. 99-110.

Evangelidis, A, Akomode, J, Taleb-Bendiab, A, Taylor, M 'Risk Assessment & Success Factors for e-Government in a UK Establishment' In *proceedings of Electronic Government, First International Conference, EGOV 2002* (eds. Traunmuller, R. and Lenk, K.) Aix-en-Provence France (2002) pp 395-402.

Evangelidis, A, Macintosh, A 'Introduction to FRAMES – An e-Government Risk Modelling Framework' In *Proceedings of the 3rd European Conference on E-Government* Trinity College Dublin Ireland (2003) pp 103-109.

Evangelidis, A., Macintosh, A., Davenport, E. 'FRAMES Towards Risk Modelling in e-Government Services: a UK perspective' *Electronic Government, Third International Conference, EGOV 2004*, Zaragoza, Spain (2004).

Frynas, G., J. 'The Limits of Globalization – Legal and Political Issues in E-Commerce*'* Management Decision, vol. 40, is. 9, (2002) pp. 871-880.

Gisler, M., Spahni, D. 'Electronic Government – Ein Űberblick' *Working Report Nr. 1*, Berner Fachhochschule Institut fur Wirtschaft and Verwaltung (2000).

Gordon, T F 'E-Government – Introduction' *ERCIM News* no. 48 (January, 2002) pp 12-13.

Greunz, M., Schopp, B., Haes, J. 'Integrating e-Government Infrastructures through Secure XML Document Containers' *Proceedings of the 34th Hawaii International Conference on System Sciences*, IEEE Press (2001).

Hoogwout, M 'Organising for Online Service Delivery: The Effects of Network on the Organisation of Transactional Service Delivery in Dutch Local Government' In *Proceedings of Electronic Government, First International Conference, EGOV 2002* (eds. Traunmuller, R. and Lenk, K.) Aix-en-Provence France (September 2-6 2002) pp 33-36.

Howard, M. 'E-Government Across the Globe: How Will 'e' Change Government?' *Government Finance Review*, issue August, (2001) pp. 6-9.

Kavan, B C, O'Hara, M T, Patterson, E C, Bostrom, R P. 'Excellence in Client/Server Information System Implementations: Understanding the STS Connection' *Management Decision* vol. 37 is. 3 (1999) pp 295-301.

Labuschagne, L., Eloff, J., H., P. 'Electronic Commerce: the Information-Security Challenge' *Information Management and Computer Security*, vol. 8, is. 3, (2000) pp. 154-157.

Laprø, L., J. 'Design Issues for Individual Online Public Services' *DEXA conference, Workshop on Electronic Government*, Greenwich, England, IEEE Press, (2000) pp. 335-339.

Layne, K., Lee, J. 'Developing fully functional E-Government: A four stage model' *Government Information Quarterly*, is. 18, (2001) pp. 122-136.

Lenk, K., Traunmüller, R. 'A Framework for Electronic Government' *DEXA conference, Workshop on Electronic Government*, Greenwich, England, IEEE Press, (2000) pp. 271-277.

Liebermann, Y., Stashevsky, S. 'Perceived Risks as Barriers to Internet and E-Commerce Usage' *Qualitative Market Research: An International Journal* vol. 5 is. 4 (2002) pp 291-300.

Papantoniou, A., Hattab, E., Afrati, F., Kayafas, E., Loumos, V. 'Change Management, a Critical Success Factor for e-Government' *DEXA conference, Workshop on Electronic Government*, Munich, Germany, IEEE Press, (2001) pp. 402-406.

Schubert, P., Hausler, U. 'E-Government meets E-Business: A Portal Site for Startup Companies in Switzerland' *Proceedings of the 34th Hawaii International Conference on System Sciences*, IEEE Press (2001).

Tchankova, L. 'Risk Identification – Basic Stage in Risk Management' *Environmental Management and Health* vol. 13 is. 3 (2002) pp 290-297.

Traunmüller, R., Lenk, K. 'E-Commerce as a Stimulus for e-Government' *13th International Bled Electronic Commerce Conference*, Bled, Slovenia, June 19-21 (2000).

Treasury Board of Canada Secretariat 'Integrated Risk Management Framework' *The TBS Web site http://www.tbs-sct.gc.ca* (2001).

