Arab Gulf Journal of Scientific Research, 25 (3): 138- 146 (2007)

Technical Paper Ref. No 2413

Risk Assessment for Implementing E-Services in some Ministries in the State of Kuwait

تقييم مخاطر تطبيق الخدمات الإلكترونية في بعض الوزارات بدولة الكويت

Abdel Nasser Hussain Zaied [1] and Faraj Al-Khairalla [2]

عبد الناصر حسين زايد وفرج الخير الله

[1] *Technology Management Program, Arabian Gulf University, Bahrain*

E-Mail: nasserhr@agu.edu.bh

[2] *Zakat House, Ministry of Awqaf, Kuwait*

ABSTRACT: The movement to e-government is basically about changing the way people and businesses interact with government. Kuwait, like any developing country, is currently launching major e-service projects aiming at improving government processes, connect government to citizens, and build interactions within the civil society. The e-services category of e-government applications enables interactions and relationships between the government and citizens, through which the latter gain access to a range of public services. However, the implementation process of e-services involves many factors of risk that could threaten the success of the process. Therefore, an effective risk management process is an important component of a successful information security program. This paper investigates and discusses the possibilities of e-services risk areas and assesses the security and privacy protection issues in some ministries in Kuwait. The results show that the total average percentage of applying security and privacy issues in the studied ministries is moderate. The Ministry of Communications (MoC) has the highest percentage of applications, whereas the Ministry of Trading and Industry (MoTI) has the lowest. Physical security is the highest applied variable, while prevention of unauthorized access is the lowest one.

Keywords: *Risk assessment, E-services, Security and privacy issues, State of Kuwait.*

المستخلص: إن التوجه نحو الحكومة الالكترونية في مضمونه يعني تغيير أسلوب تعامل المواطنين ورجال الأعمال مع الحكومة. والكويت، شأنها شأن أي دولة نامية، أطلقت مشاريع ضخمة للخدمات الالكترونية بهدف تطوير الإجراءات الحكومية وزيادة الاتصال بين الحكومة والمواطنين وبناء التفاعل داخل المجتمع المدني. إن تطبيق الخدمات الالكترونية هو أحد أنواع تطبيقات الحكومة الالكترونية الذي يُمكن الحكومة من التفاعل مع مواطنيها من خلال إتاحة العديد من الخدمات العامة. إلا أن تطبيق الخدمات الإلكترونية يحيط به العديد من المخاطر التي تهدد نجاح عملية التطبيق، وأن عملية إدارة المخاطر الناجحة تعتبر جزءاً رئيساً في برامج أمن المعلومات. يناقش هذا البحث مجالات المخاطر في تطبيق الخدمات الالكترونية بالإضافة إلى تقييم إجراءات الأمن والخصوصية في بعض الوزارات بدولة الكويت. وتشير نتائج البحث إلى أن تطبيق إجراءات الأمن والخصوصية بوجه عام في الوزارات التي تم شملتها الدراسة يتم بنسبه متوسطة، وتمثل وزارة الاتصالات أعلى نسبة تطبيق بينما تمثل وزارة التجارة والصناعة أقلها. كما أظهرت الدراسة الاهتمام بقضية الأمن المادي، وأظهرت أيضا ضعف الاهتمام بإجراءات الحماية ضد دخول غير المسموح لهم على النظم.

كلمات مدخلية: *تقويم المخاطر، الخدمات الالكترونية، قضايا الأمن والسرية، دولة الكويت.*

INTRODUCTION

The introduction of e-service solutions within the public sector has primarily been concerned with moving away from traditional information monopolies and hierarchies. E-

service remains a challenge to both citizens and public sector. The uses of Information and Communication Technology (ICT) offer significant advantages, however, it also require a much greater emphasis on security and privacy by governments, businesses, other organizations and individual users, who develop, own, provide, and manage e-services. To be successful, e-government projects must build trust within agencies, between agencies, across governments, and with businesses, NGOs and citizens (Lanvin, 2002). Trust in business-to-consumer (B2C) e-commerce is more difficult to establish than in traditional business, since there are even more barriers to overcome (Wang, 2003). The study of the trust in e-services usually focuses on issues of security and privacy in trusting the government with information provided or shared online. Trust culture refers to leadership trust, public-employee trust, and civic trust. Public-employee trust affects the response of public administration workers to the shift to e-government. Public employees may be especially threatened by online services replacing their job responsibilities. Civic trust culture refers to the pattern of behavior of the people and Civil Social Organizations (CSOs) in trusting the public, private and corporate sectors in bridging the digital divide and citizens' trust of governments in providing accurate information and using the information against them (Brown, 2002).

The problem lies on the level of security and trust offered and guaranteed by ICT providers. In this work, two risk elements (security and privacy) were discussed and evaluated in selected five Kuwaiti ministries and 11 public organizations (two in each ministry and three in ministry of awqaf). The evaluation was based on a questionnaire developed based on the terms suggested by Harvard CID (2002), APEC (2000), and NECCC (2000a, b).

RISK AREAS IN E-SERVICES

E-service can be any kind of software that offers a service to its end-users by using Internet connectivity. It relies on a permanent Internet connection and uses network-enabled smart devices as its endpoints and points of user interaction (Solange, 2004). Experience from the electronic commerce/business domain and the relevant literature shows that some researchers have attempted to classify risks in all sorts of high-level categories according to the nature of the risks. For Example, NECCC (2000b) categorized risk elements in e-commerce/e-government into eight high-level areas, as follows: 1. Leadership/Governance; 2. Privacy; 3. Security; 4. Technology; 5. Legal Readiness, 6. Customer Readiness and Accessibility; 7. Applications; and 8. Competencies.

The Treasury Board of Canada Secretariat (TBCS, 2001) classified the risks influencing an organization as follows: Political, Economical, Social, and Technological. Tchankova (2002) proposed seven different classes of risks, namely: Physical, Social, Political, Operational, Economical, Legal, and Cognitive environment. Liebermann and Stashevsky (2002) distinguished five different areas of risk in the e-commerce field, which are: i) financial, ii) physical, iii) psychological, iv) social, and v) technological.

Stoneburner, *et al.* (2001) suggested a risk assessment methodology to encompass nine primary steps, as follows: 1. System Characterization; 2. Threat Identification; 3.Vulnerability Identification; 4. Control Analysis; 5. Likelihood Determination; 6. Impact Analysis; 7. Risk Determination; 8. Control Recommendations; and 9. Results Documentation.

Evangelidis (2004) discussed the risk in e-government and provides high-level e-government risk factors classification. These factors are:

1. Societal – referring to the risks that usually affect the way people live and interact in the society;
2. 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;
3. Economical – where financial related risks are indicated;
4. 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; and

5. Security – Since security has a major importance in e-Government, projects it has to have a risk class on each own.

Furthermore, he proposed a novel risk assessment framework for e-services in the public administration.

SECURITY AND PRIVACY

The security and integrity of business transactions, privacy of data, and confidentiality of records are key concerns for citizens and businesses (IRMC, 2001). In general, "Security" is defined as protecting e-government sites from attack and misuse, while "Privacy" is defined as protecting personal information the government collects about individuals (Lanvin, 2002). The following is detailed description of each and their associated risks.

Security

Security is concerned with the protection from intended and unintended breaches that would result in the loss or dissemination of data (NECCC, 2000a). As citizens and businesses submit more information to governments over the Internet, the risk of it being stolen increases. User IDs, passwords, credit card numbers, bank account numbers, and other such data are transmitted over the Internet and stored electronically in e-government applications. The associated security risks (NECCC, 2000b) are:

- Proper authentication of parties may not exist;
- Denial of participation in transactions may occur;
- Threats exist such as viruses and hacker attacks;
- Programs or data may be introduced, modified or deleted without authorization;
- Sensitive information may be disclosed without authorization; and
- System availability may be hampered.

Privacy

The assurance that information provided for a specific transaction will not be used by the recipient for purposes not authorized by the provider. The privacy concern is: How do I know what you are going to do with my data? Governments collect information on individuals' identity and finances. Governments also collect certain information electronically from private companies. This includes statutorily required corporate filing information, tax information, and regulatory information. Governments need to protect citizens' privacy or the public may lose confidence in e-government (NECCC, 2000a). Even before the advent of e-government, some government entities made a practice of selling information about citizens. The associated privacy risks (NECCC, 2000b) are:

- Privacy policies/laws may not be consistent;
- Organizations may fail to comply with privacy policies/laws;
- Frauds such as theft of identity may occur;
- Access to data may be inappropriately granted or refused;
- Sensitive information may be disclosed without authorization; and
- Litigation and legal liability may increase.

Security and Privacy in E-services

Over the past decades, major companies have used web services (i.e. Internet-enabled services) and e-services (network-enabled services) interchangeably. E-services have different meanings to technical people and to business people. From a business context, e-services are described as an emerging paradigm that offers increased efficiency, enhanced services and stronger customer relationships through Internet-enabled applications that are reusable and customizable to user needs. From a technical point of view, standards based e-services refer to a set of programming standards that makes the interplay between different types of software over the Internet happen without human intervention (Korba, *et al.* 2006).

Brown (2002) studied the trust in e-government and focused on issues of security and privacy in trusting the government with information provided or shared online. He studied the trust culture, in assessing international, collaborative initiatives and the establishment of e-government through leadership trust, public-employee trust, and civic trust. Korba and Kenny (2002) described an architecture employing a rights management approach for the management of individual privacy rights as expressed by

European Union privacy principles. Their work goes on to provide some details as how to meet the requirements for privacy rights management (PRM).

Bellman, *et al.* (2004) examined three possible explanations for differences in Internet privacy concerns revealed by national regulation: cultural values, Internet experience and privacy preferences. They concluded that consumers in countries with sectoral regulation have less desire for more privacy regulation. Hong and Landay (2004) addressed the difficulty of designing ubiquitous software applications that are privacy-sensitive or that help the user to manage his/her privacy. Yee and Korba (2004) examined how an e-service client can be assured that the e-service provider with whom he/she is interacting complies with his/her privacy policy. The client's privacy policy specifies what private information the client is willing to give up and the conditions for access to the information (e.g., the provider can only have access during week days). The provider's privacy policy specifies what private information the service requires and the conditions that govern the provider's access to the information. The e-service can only be engaged if the client's privacy policy matches the provider's privacy policy.

Asgarkhani (2005) studied some of the key aspects of electronic government and e-Service. He examined the value and the effectiveness of e-Services within the public sector with a focus on four specific facets of effectiveness. These are: the view of management and ICT strategists; social, cultural and ethical implications; the implications of lack of access to ICT; and the customers'/citizens' view of the usefulness and success of e-Service initiatives. Farahmand, *et al.* (2005) provided a management perspective on the issues related to security in e-commerce, the important issues confronting managers, security enforcement measure/techniques, and potential threats and attacks. They also developed a scheme for probabilistic evaluation of the impact of security threats that might be used to assess the probability of success of attacks on information assets in organizations, and to evaluate the expected damages of these attacks.

Korba, *et al.* (2006) described some of the driving forces and approaches for the development and deployment of privacy architectures for e-services, as well as presented several privacy information flow scenarios that can be applied for assessing privacy architectures.

Security and Privacy Assessments

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. Risk analysis is a method of identifying vulnerabilities and threats, and assessing the possible damage to determine where to implement security and privacy safeguards (Stoneburner, *et al.* 2001).

METHODOLOGY

The methodology used for this analysis consisted of a survey in organizations from five Kuwaiti ministries. A questionnaire was distributed and follow-up interviews conducted with at least two members in each organization. In a few cases more than two members from the participating organization were interviewed. All the interviews were conducted in a face-to-face setting in the location of the interviewee's workplace. The duration of the interviews ranged from few minutes to half an hour. Although data collection was made mainly through semi-structured interviewing, additional data was obtained through study of websites, and various other secondary sources.

Assessment Tool

In this study, a questionnaire developed based on the terms suggested by Harvard CID (2002), APEC (2000) and NECCC (2000a, b) was distributed. The questionnaire consisted of 18 questions to investigate the participants' opinions towards the security and privacy issues in their organizations. The questionnaire contents are listed in Table 1.

Table 1. Questionnaire Content.

1.	A formal system/application development methodology, designed for e-government, is used for all Information and Communications Technology (ICT) projects.
2.	We have the technological infrastructure and competencies to effectively engage in e-government initiatives.
3.	E-government systems are comprehensively and regularly tested and reviewed to provide assurance that controls are present and effective.
4.	On going monitoring is performed to ensure that unauthorized system changes have not occurred.
5.	E-government system changes are properly authorized and tested sufficiently.
6.	The organization's disaster recovery planning deals with e-government issues, and is reviewed regularly
7.	Individual access to systems and information is properly controlled.
8.	There is a system in place to recognize security gaps.
9.	Security policies, plans and procedures are documented and shared with personnel and third parties that have access to systems, data or facilities.
10.	An information systems security manager has been nominated and is carrying out activities in accordance with government guidelines.
11.	Risk assessments for information are regularly performed to respond to changes to the system or operating environment.
12.	Security is a shared responsibility within the organization, and personnel are held accountable for it.
13.	Ongoing security training is conducted for all relevant personnel.
14.	Effective techniques are in place to offer protection from threats, including viruses, and hackers.
15.	Our organization is sensitive to customer concerns about privacy, confidentiality and security, and addresses them by complying with clear policies and guidelines on these topics.
16.	Effective techniques are in place to allow secure communication across the Internet, protecting the traffic from inappropriate leak or modification.
17.	There are Security policies, plans and procedures applied strictly within the organization.
18.	Our Internet solutions are flexible to contain rapid change and scalability.

Participants were asked to indicate the extent of their agreement or disagreement on a five-point Likert-type scale. i.e., Completely Agree – Agree - Don't know – Disagree - Completely disagree (Schmeiser and Deutsch, 1977).

The eighteen questions covered five main variables, as follows:

- Physical security (Questions 2, 4, 5, 7, 8, 13, 16, 17 and 18).
- Protection of information, which includes periodic backup and offsite rotation of mission critical systems, applications, and data (Questions 1, 3, 4, 9, 10, 11, 12, 14, 15, 16 and 17).
- Prevention of unauthorized access (Questions 1, 3, 4, 5, 7, 10, 11, 12 and 13).
- Detection of security breaches (Questions 3, 6, 7, 8, 9, 10, 11, 14, 16 and 18).
- Procedures for reporting security breaches to management or appropriate authority (Questions 1, 2, 8, 9, 10 and 12).

Sample Size

Existing plans for offering e-services and available infrastructure have been applied to select the ministries under study. Three criteria, percentage of expenditures on IT, percentage of IT staff, and percentage of employees using computers, were applied to select the participant organizations. Fifteen public organizations stated that they have a plan for e-government applications. The range for applying these plans is between 3 to 10 years. Eleven public organizations in five ministries were selected and the sample was made up of employees from these organizations. The percentage of Internet users within the selected organizations was 66.2%, with 72.5% of these organizations have more than 70 PCs per 100 of their employees. A total of 220 copies of the questionnaire were distributed (20 for each organization).

Data Collection

As a result of distributing questionnaires and conducting personal interviews, one hundred and six questionnaires were received (49%). The respondents' classification is shown in Table 2.

Table 2. Number of Questionnaires Received.

Ministries	Number	Percentage
Ministry of Communications (MC)	21	53 %
Ministry of Trading and Industry (MTI)	21	53 %
Ministry of Education (ME)	21	53 %
Ministry of Awqaf and Islamic Affairs (MAIA)	28	47 %
Ministry of Finance (MF)	15	38 %
Total of participants	**106**	**49%**

RESULTS AND DISCUSSION

Assessment Results

To assess the appropriateness of security and privacy issues in Kuwaiti ministries under study, the average of the "completely agree" and "agree" answers were taken. The results show that the average of participants' agreements regarding to applying security and privacy issues in Kuwaiti ministries under study is 54%, whereas 22% don't know and 34% disagree or completely disagree as shown in Table 3.

The participants' opinions towards applying security and privacy issues are shown in Table 4, (MC) has the highest percentage (64%), whereas (MTI) has the lowest percentage (38%).

Analysis and Discussion

Analysis of the results indicated that participants have positive perception about the relative importance of security and privacy within their organizations. Thus, the majority of the survey participants perceived that their organizations have effective techniques to offer protection from threats, including viruses, and hackers, and that individual access to systems and information is properly controlled. These perceptions towards the study variables vary from ministry to another as follows:

Analysis Regarding to the Whole Ministries

The participants agreed that:

a- "The organization's disaster recovery planning deals with e-government issues and the ongoing security training" are insufficient and applied only with (43%);

b- "The individual access to systems and information" is properly controlled by (66%); and

c- "The effective techniques are in place to offer protection from threats, including viruses, and hackers" by (73%).

Table 3. Participant's Answers.

Completely Agree	Agree	Don>t know	Disagree	Completely disagree
16%	38%	22%	14%	10%

Table 4. Percentage of Applying Security and Privacy Issues in Kuwaiti Ministries.

Q. No.	MoC (21)	MoTI (21)	MoE (21)	MoA (28)	MoF (15)	Av.%
1	0.71	0.43	0.48	0.57	0.47	**0.53**
2	0.52	0.29	0.48	0.82	0.67	**0.56**
3	0.48	0.48	0.43	0.39	0.47	**0.45**
4	0.62	0.43	0.71	0.50	0.67	**0.59**
5	0.57	0.33	0.48	0.43	0.40	**0.44**
6	0.52	0.29	0.48	0.46	0.40	**0.43**
7	0.81	0.62	0.48	0.71	0.67	**0.66**
8	0.62	0.38	0.48	0.61	0.53	**0.52**
9	0.57	0.29	0.48	0.43	0.67	**0.49**
10	0.62	0.33	0.62	0.39	0.40	**0.47**
11	0.52	0.38	0.38	0.39	0.53	**0.44**
12	0.67	0.48	0.52	0.61	0.73	**0.60**
13	0.48	0.38	0.38	0.36	0.53	**0.43**
14	0.86	0.43	0.67	0.82	0.87	**0.73**
15	0.67	0.33	0.67	0.57	0.87	**0.62**
16	0.81	0.29	0.57	0.54	0.80	**0.60**
17	0.76	0.33	0.71	0.68	0.73	**0.64**
18	0.67	0.33	0.67	0.54	0.67	**0.58**
Av.%	**0.64**	**0.38**	**0.54**	**0.55**	**0.61**	**54%**

Analysis Regarding to Individual Ministries

According to participants' agreements, the highest agreement is 87% in (MF) and lowest agreement is 29% in (MTI) as shown in Table 4.

Analysis Regarding to Variables

The questions on each of the five variables were grouped. The results show that there is a significant variation in trust of applying these variables among the same ministry. The

Table 4. Participant's Answers.

Ministries			Highest agreement	Lowest agreement
Ministry of Communications	Question(S)		• Effective techniques are in place to offer protection from threats, including viruses and hackers.	• E-government systems are comprehensively and regularly tested and reviewed to provide assurance that controls are present and effective. • Ongoing security training is conducted for all relevant personnel.
	%		86	48
Ministry of Trading and Industry	Question(S)		• Individual access to systems and information is properly controlled.	• We have the technological infrastructure and competencies to effectively engage in e- government initiatives. • The organization's disaster recovery planning deals with e-government issues, and is reviewed regularly. • Security policies, plans and procedures are documented and shared with personnel and third parties that have access to systems, data or facilities. • Effective techniques are in place to allow secure communication across the Internet, protecting the traffic from inappropriate leak or modification.
	%		62	29
Ministry of Education	Question(S)		• Ongoing monitoring is performed to ensure that unauthorized system changes have not occurred • There are security policies, plans and procedures applied strictly within the organization.	• Security is a shared responsibility within the organization, and personnel are held accountable for it. • Ongoing security training is conducted for all relevant personnel.
	%		71	38
Ministry of Awqaf and Islamic Affairs	Question(S)		• We have the technological infrastructure and competencies to effectively engage in e-government initiatives. • Effective techniques are in place to offer protection from threats, including viruses, and hackers.	• Ongoing security training is conducted for all relevant personnel.
	%		82	36
Ministry of Finance	Question(S)		• Effective techniques are in place to offer protection from threats, including viruses, and hackers. • Our organization is sensitive to customer concerns about privacy, confidentiality and security, and addresses them by complying with clear policies and guidelines on these topics.	• E-government system changes are properly authorized and tested sufficiently. • The organization's disaster recovery planning deals with e-government issues, and is reviewed regularly. • An information systems security manager has been nominated and is carrying out activities in accordance with government guidelines.
	%		87	40

variation within the ministries ranged between 5% as in (MC) and 10% as in (MA). Among all the ministries, it ranged between 18% as in "Prevention of unauthorized access" and 28% as in "Protection of information", as shown in Table 5. The variables of Physical Security and Protection of Information are the highest applied variables with a percentage of 56%, while the lowest variable is Prevention of Unauthorized Access at 51%.

Table 5. Percentage of Applying Security and Privacy Variables.

Variables	(MC)	(MTI)	(ME)	(MAIA)	(MF)	Av.%
Physical security	65%	38%	55%	58%	63%	**56%**
Protection of information	66%	38%	57%	54%	65%	**56%**
Prevention of unauthorized access	61%	43%	50%	48%	54%	**51%**
Detection of security breaches	65%	38%	52%	53%	60%	**54%**
Procedures for reporting security breaches	62%	37%	51%	57%	58%	**53%**

CONCLUSION AND RECOMMENDATIONS

Some organizations in kuwait use web servers to provide information or services to the public. These Web servers are typically considered to have greater risk because at any point along the connection, network traffic can be monitored. Attackers who are able to compromise one of these systems on the network might use that compromised system to gather any confidential information about the user.

From the study results, it can be concluded that the total average percentage of applying security and privacy issues in the studied Kuwaiti ministries is moderate. The Ministry of Communications has the highest percentage of applications, whereas the Ministry of Trade and Industry has the lowest. Physical security is the highest applied variable, while prevention of unauthorized access is the lowest applied. Organization's disaster recovery planning deals with e-government issues and the ongoing security training have insufficient applications (43%). On the other hand, individual access to systems and information is properly controlled (66%), and effective techniques are in place to offer protection from threats, including viruses and hackers (73%). Physical security and protection of information are the highest applied variable with a percentage of 56%, and the lowest applied variable is prevention of unauthorized access (51%).

FUTURE WORK

The e-services risk areas in public organizations in the State of Kuwait is still not clear due to the inclusion in this study of only two variables. More investigations are needed to study other variable, such as information security, management skills and leadership. In addition, successful implementation of e-government strategies requires the establishment of special e-culture as an important component of these strategies.

REFERENCES

APEC (2000) *E-Commerce Readiness Guide, Electronic Commerce Steering Group*, Asian Pacific Economic Cooperation *(APEC)*. Available at: www.ecommerce.gov/apec

Asgarkhani, M (2005) The Effectiveness of e-Service in Local Government: A Case Study. *The Electronic Journal of e-Government,* **3**(4):157-166.

Bellman, S, Johnson, E, Kobrin, S, and **Lohse, G** (2004) International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society,* **20**(5): 313-324.

Brown, CL (2002) G-8 Collaborative Initiatives and the Digital Divide: Readiness for e-Government. *In*: *Proceedings of 35th Hawaii International Conference on System Sciences*, pp. 1-10.

Evangelidis, A (2004) FRAMES – A Risk Assessment Framework for e-Services, *Electronic Journal of E-Government,* **2**(1): 21-30.

Farahmand, F, Navathe, S, Sharp, G, and **Enslow, P** (2005) A Management Perspective

on Risk of Security Threats to Information Systems, *Journal of Information Technology and Management,* **6**(2/3): 203-225.

Harvard CID (2002) *Global Information Technology Report; Readiness for the Networked World 2001-2002 and 2002-2003.* Center for International Development, Harvard University, USA. Available at www.weforum.org/gitr and at: www.readinessguide.org

Hong, JI and **Landay, JA** (2004) An Architecture for Privacy-Sensitive Ubiquitous Computing. *Proceedings of Second International Conference on Mobile Systems, Applications, and Services (MobiSys 2004)*, 6-9 June 2004, Boston, UK.

IRMC (2001) E-Government: using Technology to Transform North Carolina's Governmental Services and Operations in the Digital Age, North Carolina Governmental Report, Information Resource Management Commission, USA.

Korba, L and **Kenny, S** (2002) *Towards Meeting the Privacy Challenge: Adapting DRM, DRM 2002,* Washington, D.C.

Korba, L, Song, R, and **Yee, G** (2006) *Privacy Management Architectures for E-Services,* National Research Council Canada, NRC 48271, Canada.

Lanvin, B (2002) *E-government Handbook for Developing Countries.* The World Bank, USA.

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

NECCC (2000a) Critical Business Issues in the Transformation to Electronic Government. The National Electronic Commerce, December 2000. Available at: www.ec3.org, 2/7/2006

NECCC (2000b) Risk Assessment Guidebook for E-Commerce/e-Government. The National Electronic Commerce. Available at: www. ec3. org, 19/4/2004

Schmeiser, BW, and **Deutsch, SJ** (1977) Quantile Estimation from Grouped Data: the Cell Mid Point. *Communications in Statistics: Simulation and Computation,* **6B** (3): 221-234.

Solange Ghernaouti Hélie (2004) Increase Trust and Confidence in Information and Communication Technologies by Multidisciplinary Approach. *In: Proceedings of XIV E Conference RESER, 23- 24 September* 2004, Castres.

Stoneburner, G, Goguen, A, and **Feringa, A** (2001) *Risk Management Guide for Information Technology Systems.* National Institute of Standards and Technology, Special Publication 800-30, U.S. Government Printing Office, Washington, USA.

Tchankova, L (2002) Risk Identification: Basic Stage in Risk Management. *Environmental Management and Health,* **13**(3): 290-297.

TBCS (2001) Integrated Risk Management Framework. Treasury Board of Canada Secretariat, Canada Available at: ww.w.tbs-sct.gc.ca.

Wang, M (2003) Assessment of E-Service Quality via E-Satisfaction in E-Commerce Globalization. *The Electronic Journal on Information Systems in Developing Countries (EJISDC),* **11**(10): 1-4.

Yee, G, and **Korba, L** (2004) Privacy Policy Compliance for Web Services. *In*: *Proceedings of IEEE International Conference on Web Services (ICWS 2004)*, San Diego, California, USA.

Ref. No. (2413)
Rec. 18 / 01/ 2007
In-revised form 04 / 10/ 200