

## **Combining the ISO/IEC 27001 international standard and total quality management to ensure successful electronic Government**

Prof.Dr.Sherif.A.Elaraby

Deputy Director General for Quality Assurance,  
Dean of Productivity and Quality Institute, Academy for Science and Technology,  
P.O. Box 1029, Alexandria, Egypt. E-mail: sh\_araby@aast.edu

A. Elkashlan<sup>#</sup>, Academy for Science and Technology, P.O. Box 1029, Alexandria,  
Egypt. E-mail : kashlan@aast.edu <sup>#</sup> (corresponding author)

Key words: e-government; total quality management; security; ISO/IEC 27000 standard.

### **Abstract**

The transition from conventional government services to electronic government services is becoming an international trend. The transition provides benefits not only to the government, but also to all organizations and people. The transition is also an opportunity for the government to recognize its services and eliminate unnecessary overheads that may exist in its traditional services.

The purpose of the present paper is to highlight the importance of adopting total quality management concepts to assist electronic government to continually improve services to citizens. Success of e-government depends upon the development and sharing of a wide variety of standards. The paper includes a brief framework for the electronic government and presents the benefits, management readiness, sensitivity to cost through adopting total quality management concepts. The main goal is to investigate the synergistic relationship between electronic government performance and the international standard ISO/ IEC27001, entitled information security management standard (ISMS). Agencies that do not provide an appropriate security environment for their information assets place at risk the government at large, not just themselves. It is expected that Integrating total quality management concepts with ISO/IEC 27001 international standard assist in improving the performance of the electronic government, achieve the targeted democracy, and continually improves the government performance in diverse areas, as continual improvement is intrinsic within the standard.

## Introduction

Electronic government (e-government) is employed as a tool for supporting better government administration and public services.

E-government represents a new role for information more responsive to citizens. E-government is not an aim in itself; it is often considered "e-business of the state". It is about a process of reform in the way governments work, share information and deliver services to external (citizens) and internal clients for the benefit of government, citizens and businesses that they serve. Moreover, e-government harnesses information technology such as wide area network (WAN), internet, world wide web (WWW), and mobile computing by government agencies to reach out to citizens, business, and other arms of the government to improve delivery of services to citizens, improve interface with business and industry, empower citizens through access to knowledge and information, and make the working of the government more efficient and effective.

Although there are plenty definitions of e-government based on the general five dimensions (Technological; Legal; Democratic; Organizational; Socio-economic) the major actual government's objectives are indisputable: maintaining collective security, administering justice. The resulting benefits could be more transparency, greater convenience, less corruption, revenue growth, and cost reduction for both the government itself and the adopter of e-government services (Gronlund, 2002). Furthermore, more public agencies have employed the statistical analysis and data networks that make it possible to create information- based innovations. They have moved beyond manual (traditional) government and e-government to what is truly innovative information government (I-government). Obviously, the phrase "e-government" covers a variety of different public sector activities that are enhance or permitted by data processing capacity. The most known distinct categories are (1) e-government information makes existing information more widely available to citizens by putting it on the internet. (2) e-government automation converts manual work to electronic work. (3) e-government reengineering is the radical redesign of an important but existing process. It has a fundamental impact on how services are delivered, how public policies are developed. (4) I-government innovation begins by automating or redesigning existing work.

Instead, I-government is a completely unprecedented strategy for a public purpose. The innovation lies in the novel use of the information that the electronic technology makes possible. Generally, to move from manual (traditional) government to e-government requires more automation, to move from e-government to I-government however, requires true innovation. The slow spread of e-government services include inertia, security and confidentiality, lack of computer skills, difficulties in carrying our organizational change, and the nature of public sector financing and procurement practices (World Bank,2003). While a significant body of academic literature exists on e-government services, work on e-government up to date, has focused on the supply side, in particular, most at success factors and impediments of e-government initiatives (Jaeger,2009; Lowe, 2003), models of e-government evolution and growth (Reddic,2004;West,2004), as well as practices, effectiveness of implementation and challenges of e-government services(Jaeger and Thompson,2003;Moon,2002). Electronic public services delivery is the most extended strategy for e-government development. The Internet is considered as a mean to transform the understanding of interactions with citizens and the participation of public affairs. In this regard, it was

suggested the extension of democratic processes and promotion of democracy, including consultation in the decision-making process, free flow of information, possibility of consulting government statistics data, and participation in elections of representatives (Hacker and Van Dijk, 2000). The e-government at the local level may be classified in different ways depending on the criteria used. From a relational viewpoint these are:- Authority –to- citizen e-government (A2C), Citizen –to- authority e-government (C2A), Authority-to-authority e-government (A2A), Business-to-authority e-government (B2A), authority-to-business e-government (A2B). While from functional point of view, local e-government can be divided into two main areas: use ICT's in performing basic administrative, service and democratic tasks on the one hand, and strategic information system development policies and relates citizen/user-oriented assessment, on the other hand.

### **Quality measures**

Quality issue has become an increasing area of interest within the digital age. The debate on the value, or otherwise, of quality management system in improving service has a long history.

Quality management has become a major issue for business worldwide. Many studies have highlighted the importance of total quality management (TQM) for organizations, it has been widely implemented, and Organizations have arrived at the conclusion that effective (TQM) implementation can improve their competitive abilities and overall business performance (Anderson et al, 2007).

Governments are becoming aware of its effectiveness as a management framework that supports its performance and made to be applicable to the entire management and in any branch of business. The framework principles are summarized in three pillars: customer focus, people involvement and continuous improvement. Adoption of (TQM) principles creates organizational culture that facilitates the implementation of e-government and views its citizens as partners. In fact quality management calls for the use of a set of mechanisms to collect and analyze customer feedback from its environment (internal and external) which are essential to design effective and easy-to-use e-services. Moreover, the higher management readiness, the more likely the government will adopt (TQM). And the higher the sensitivity to cost, the more likely the government adopt both (TQM) and e-government services. Governments adopting (TQM) concepts are struggling to meet citizen's expectations especially under intensified pressure to reduce costs and reduce budgets. The greater the external pressure faced, the more likely the government will adopt (TQM) for continuous improvement of e-services.

The success of e-government is depending on its quality and usage. The higher the government quality, the better services are provided. Generally the four significant quality aspects for the e-government are: Information quality, system quality, Service quality, and software quality.

### **E-government principles**

E-government and all agencies must provide the conditions needed to conserve information privacy of citizens, companies, and all users, respecting and complying with the legislation that establishes the restrictions on access.

Successful services to citizens are built on an understanding of their needs. The key challenges facing e-government delivery are the provision of a unified public interface

to government information and services, balance between protecting citizen's rights, and better matching their needs with efficient, integrated, engaging processes. Besides, a number of vital challenges that have to be addressed namely, financial barriers, technology change, digital divide, and legislative barriers (Gronlund, 2002 ). Overcoming these challenges require information management and cooperation among government departments to consolidate and redefine current work processes and structures. Despite e-government requires considering information as a strategic resource for all government activities, there is no agreement on what constitutes effective information quality criteria. E-government functions best when all levels work seamlessly together and invites its citizens to behave as partners. The seven principles of e-government stated and approved universally are (Great Britain cabinet office, 1998)

1-**Choice**- make electronic delivery of services the preferred option.

2-**Confidence**- safeguard information collected from citizens and business and ensures citizens are made aware of this safeguarding.

3- **Accessibility**- provide services in a format that customer requires them, paying special attention to the needs of people in remote areas, people with limited mobility, and people who do not speak the country's official language(s).

4- **Efficiency**- streamline, automate and integrate government processes so that the boundaries between government departments are invisible or irrelevant to the user, perhaps beneficial interactions.

5- **Rationalization**- share resources for functions and processes which are common to more than one department or agency.

6- **Open information**- make information readily available in convenient and useful forms.

7- **Fraud protection**- establish measures which check the identity of individuals and organizations dealing with government and to ensure that information cannot be incorrectly accessed or manipulated.

This protection is achieved via ISO/IEC 27001 standard as a key factor with a goal to help distinguish official sources from non-official ones which could be providing misinformation. The use of such common standard and guideline builds the capacity for interoperability between agencies and assists with achieving a consistent application of information security.

Surprisingly little is known about the reasons for low adoption of ISO/IEC 27001 series of standards published in October 2005 by the international organization for standardization (ISO) and the international electrotechnical commission (IEC), entitled *ISO/IEC 27001:2005- information technology-security techniques-information security-management systems (ISMS)- requirements*, and it is commonly known as ISO/IEC 27001:2005. The standard has been developed for protecting organization's (government's) information assets. Several national bodies expressed the opinion that the standard has already proven entirely adequate for government use. The standards are the product of ISO/IEC JT (Joint Technical committee 1) SC27 (sub committee 27), an international body that meets in person twice a year. The standard provides best practice recommendation on information security management, risks and controls within the context of an overall information security management system (ISMS). It is similar in design to management systems for quality assurance (ISO9000 series) and environmental protection (ISO14000 series).

## **Barriers and sources of failure for e-government**

All information on the internet is subject to interception, security and privacy have been considered as main barriers to e-government. Barriers include lack of clear vision or goal of the electronic solution; a lack of coherent leadership; a lack of information technology skills in e-government workforce; poor communication and training of e-government staff; a tendency to ignore human factors in design of electronic solutions; and loss of expertise to design and streamline e-government processes.

Applying total quality management concepts and the ISO/IEC 27001 international standard resolves most of these barriers.

## **Diffusion of ISO 9001, ISO 14001, and ISO/IEC 27001 standards**

The publications dedicated to ISO/IEC 27001 standard and its diffusion, is not taking place at the expected rate despite the high interest in the ISMS topic triggered by the interest in investing in this phenomenon (Weick, 1989). The success of global diffusion of two series of management system standards (MSS) for quality management and environmental management (Whitelaw, 2004) inspired the international organization for standardization to publish a series of information security management system standards including the standard ISO/IEC 27001:2005.

The publication is intended to offer the global markets a possibility for harmonizing diverse information systems (IS) security methods and methodologies by adopting the newly published one. The ISO 9000 series for quality management standards, the ISO 14000 environmental management system, and the ISO/IEC 27001 information security management standards all have much in common (Brewer and Nash, 2005). First they are built on the several Plan-Do-Check-Act (PDCA) process cycle model, which specifies the requirements and processes to enable a business to establish, implement, review and monitor, manage and maintain effective management system, whether it be quality, environmental, or information security management (Humphreys, 2005). Second, they are made to complement one another in a way to enable organizations (governments) create an integrated management system, i.e., a single management system that compiles with more than one management standard (Brewer and Nash, 2005). Third, due to the correspondence between ISO 9001, ISO 14001, and ISO/IEC 27001 it makes it easier for governments that have experience with one standard to implement another one. Fourth, all the three management systems standards (MSS) can be certified. Certification is not mandatory, but most organizations that implement the standard also go for a certificate for its positive impact on business, the process of creation of products and services can be managed using a system. Overall, the positive effects of stemming from certification should outweigh the high cost of (MSS) implementation and certification (Delmas, 2002). However information security management system certification is considered as leverage for confidence between government departments from one side and citizens engaged in business transactions from other side.

## **Relationship ISO/IEC 27001, ISO/IEC 27002**

Without information security, the business is faced with negative impacts including financial consequences, weakened protection of both government's human resources capital i.e. knowledge, loss of market share, poor performance ratings,

ineffective operations, inability to comply with laws and regulations, or loss of image and reputation (Humphreys, 2006).

The standard ISO/IEC27001 formally defines mandatory requirements for an information security management system (ISMS).It uses ISO/IEC27002 to indicate suitable information security controls within the ISMS.

### **ISO/IEC 27002:2005 – the current, issued standard**

ISO/IEC 17799:2005 was renumbered ISO/IEC27002:2005 in the middle of 2007 to bring it to the ISO 27000 family of standards.

ISO/IEC27002:2005, the latest version of "*information technology-security techniques-code of practice for information security management*" is considered absolutely essential in the use of ISO/IEC 27001.It is a normative reference, advisory document and explicitly concerned with information security assets. The standard is a revised version of the version first published by ISO/IEC in 2000, which was a word-for-word copy of the British standard (BS 7799-1:1999). Information security is defined within the standard in the context of the C-I-A triad:

-Confidentiality (ensuring that information is accessible only to those authorized to have access via authentication, provide an easier, smarter, faster way for citizens to get the services and information they want).

-Integrity (safeguard the accuracy and completeness of information and processing methods for secure online transactions and trustworthy technology).

-Availability (ensuring that authorized users have access to information and associated assets when required).

### *Contents (Outline) of ISO/IEC27002*

ISO/IEC 27002 is a code of practice-a generic, not truly a standard; it lays out a structured set of suggested controls.

Despite the present paper is not focusing on ISO/IEC 27000 series yet the main sections and contents that applicable to e-government are mentioned in brief.1)risk management 2)security policy-management direction 3)organization of information security –governance of information security 4)assets management-inventory and classification of information assets 5) human resources security- security aspects for employees joining, leaving, moving and leaving government 6)physical and environmental security-protection of the computer facilities 7)communications and operations management- management of technical security controls in systems and networks 8)access control- restriction of access rights to networks, systems, applications, functions and data 9)information systems acquisition, development and maintenance-building security into applications 10)information security incident management- anticipating and responding appropriately to information security breaches 11)business continuity management-protecting, maintain and recovering business-critical processes and systems 12)compliance-ensuring conformance with information security policies, standards, laws and regulations (Humphreys,2006).

ISO/IEC27002 is currently under revision, numerous comments and improvement suggestions were discussed at the ISO/IEC JTC1/SC27 meeting in Beijing in May 2009.

### **Conclusion**

The term e-government covers several aspects of managing government. The definition adopted in the present paper revolves around the way for governments to use the new information and communication technologies to provide people with more convenient access to government information and services, to improve the quality of services, and to provide greater opportunities to participate in democratic institutions and processes. E-government employs information technology to conduct operations and to interface with citizens. Operations must be conducted securely, accurately, and protected from unauthorized disclosure. Designing web sites that are responsive to citizens' needs shares for the success of online services. Government should manage the acquisition, management and maintenance of information in accordance with a quality assurance plan whilst reducing the cost of doing so. Use of the ISO/IEC 27001:2005 international standard enables governments to achieve these goals, protect and maintain citizen's privacy, enhances information quality assurance, and maximizes these activities using proven management framework such as total quality management together with full conformance with the security standard. The impact of combining ISO/IEC 27001 and total quality management is positive not only from a technological point of view, but specially for the behavior of citizen's i.e. social and economic consequences. We do not yet have good measures for e-government performance or agreement on what should be measured. Despite e-government requires considering information as a strategic resource for all government activities, there is no agreement on what constitutes effective information quality criteria. The total quality management principles and the ISO/IEC2700 standard are appropriate in this context. Finally it should be noted that the technology of hacking has been increasing steadily despite increased security issues, and the cycle continues.

## References

- Ake Gronlund, (2002), *Electronic Government: Design, Applications and Management*. Ideal group publishing, USA.
- Anderson, E.W., Fornell, C. and Lehmann, D.(2007),"Customer satisfaction, market share, and profitability" *Journal of marketing*, Vol.58, July, pp.53-56.
- Brewer, D. and Nash, M. (2005),"the similarity between ISO9000 and BS 7799-2", Gamma Secure Ltd.
- Delmas, M.A.(2002),"The diffusion of environmental management standards in Europe and in the United States: an institutional perspective", *Political sciences*,35,91-119.
- Great Britain cabinet Office (1998).*Electronic government: The view from the queue: comprehensive research into potential customer take-up of online government services*.
- Hacker, K. Kennent, L. Jan van Dijk (editors) 2000,"*Digital Democracy, issues of theory and practice*" Sage London.
- Humphreys, T (2005),"State-of- the –art information security management system with ISO/IEC 27001", *ISO management systems*, pp15-18.
- Humphreys, T (2006),"State-of- the –art information security management system with ISO/IEC 27001", *ISO management*

- systems, Special report, pp9-13.
- Jaeger, P.T. (2003), "The endless wire: E-government as global phenomenon", *Government Information Quarterly*, 20, pp.323-331.
- Jaeger, P.T., Thompson, K.M. (2003) "E-government around the world: lessons, challenges, and future directions", *Government Information Quarterly*, 20, pp.389-394.
- Lowe, C. (2003), "Experiences of take-up of e-government in Europe", *Lecture notes in Computer Science* 2739, pp. 160-163.
- Moon, M.J.(2002), "The evolution of E-government among municipalities: rhetoric or reality?", *Public administration review*, 42 (4), pp.424-433.
- Reddic, C.G. (2004), "A Two-state model of E-government growth: Theories and empirical evidence for US cities " *Government Information Quarterly*, 21, 51-64.
- The World Bank, South Asia component, Annual book conference on department economics, Bangalore, May 2003.
- Weick, K.E.(1989), "Theory construction as disciplined imagination", *Academy of management review*, 14 (14), pp.516- 531.
- West, D.M.(2004) , "E-government and the transformations of service delivery and citizen attitudes", *Public administration review*, 64 (1), pp.15-27.