

# Knowledge Management in E-Government



**Deborah S. Carstens**

*Florida Institute of Technology, USA*

**LuAnn Bean**

*Florida Institute of Technology, USA*

**Judith Barlow**

*Florida Institute of Technology, USA*

## INTRODUCTION

Over the past decade, government has created innovative and complex systems connecting people to information by focusing on Knowledge Management (KM) practices. KM, described as the comprehensive management of an organization's expertise through collecting, categorizing and disseminating knowledge, leads to knowledge discovery through techniques such as data mining. These developments have transformed traditional access to public services into e-government. Ever increasing demand to access and information has also brought about e-government policy development challenges for integrative KM practices in public services (Riege & Lindsay, 2006). In particular, the size and complexity of governmental structures and the vast data stores have become problematic (Koh, Ryan, & Prybutok, 2005). Because government uses, collects, processes, and disseminates sensitive information containing personal, financial and medical data, it is very easy for organizations to reprocess the information and disseminate it (Hewett & Whitaker, 2002). Ebrahim and Irani (2005) state that the benefits gained by data mining and KM practices are erased when information is not viewed as confidential but instead as a commodity to be bought and sold. Therefore, e-government must uphold a higher standard of ethics in KM practices through continued development of codes of conduct and governance policies for data that build citizen trust and ensure success of e-government services and transactions (Verschoor, 2000). An excellent framework to effectively preserve this trust is a balanced scorecard (BSC), which was first introduced by Kaplan and Norton (1992, 1996a, 1996b). The framework serves to continuously improve the KM process when modified for e-government. Therefore, this chapter describes technological and organizational challenges faced by e-government in KM and retrieval and presents the BSC framework to overcome these challenges.

## BACKGROUND

Government information systems have proved to be an efficient way to facilitate communication, provide information and deliver services to citizens. While database management systems lead to better data capture, storage, processing and sharing capabilities, extracting useful information from the data presents adversities for government (Robertson & Powell, 1999).

Electronic data capture and storage for later retrieval are major expenses associated with successful data mining applications (Robertson & Powell, 1999). Knowledge capture results from the use of data sources to find intelligent patterns in the data. The increase in the number existing government e-commerce sites that have the means to capture citizen data greatly reduces the cost of starting a data mining application (Tan, Steinbach, & Kumar, 2006).

Data mining software applies complex algorithms to massive data stores important for discovering relationships (Turban, Leidner, McLean, & Wetherbe, 2006). Within the public sector, data mining methods yield powerful information about the interrelationships between data elements (Robb & Coronel, 2006). Likewise, rich opportunities exist for uncovering "new" intelligence in government information.

While data mining technology advances, the potential impacts of mining citizens' private data present legal, social and ethical questions (Taipale, 2007). In addition to privacy, inherent risks of accuracy and integrity can result when data is merged from multiple sources. Safeguards for addressing privacy and integrity risks include formal codes of ethics, written ethics policies mandated employee training, and even audits that flag unauthorized access to data (von der Embse, Desai, & Desai, 2004). More specifically, legislators have enacted laws and regulations to protect citizen data (Glover & Owen, 2004). These include the Gramm-Leach-Bliley Act for financial data, Children's Online Privacy Protection Act for use/collection of child data online, the Electronic Communications Privacy Act, Privacy Act, Cable Communications Policy Act, and HIPAA regulations regarding medical information.

From a risk perspective, numerous technologies utilized in the e-government environment, as well as process/user interactions and system compatibility issues must be evaluated as potential areas of misuse or impediments. Technologically, the maze of perspective subcategories such as m-government (mobile government), u-government (ubiquitous government), and g-government (government GIS/GPS applications) provide complexities that are not much different from public sector information portals (Riley, 2007). However, the highly private nature of the data, ethical questions about its ownership, and IT infrastructure makes the stakes higher in an e-government configuration (Taipale, 2003).

From a process interaction perspective, risks can arise from the following types of systems: Government-to-Citizen (G2C), Government-to-Business (G2B), Government-to-Government (G2G) or Government-to-Employees (G2E) (Turban et al., 2006). For example, G2C systems support the majority of citizen data captured, including online systems for driver license renewal, vehicle tag renewal, voter registration, social benefits management, court records, and state property appraisal information. Despite the highly personal and private nature of G2C Web site exchanges, the G2B systems, which interface with business information systems, open even a more complex Pandora's Box of data security and data access solutions (Sagheb-Tehrani, 2007). G2G systems linking governments face problems with inconsistent policies/laws, intergovernment or interagency politics, language barriers, and customs (Jing & Pengzhu, 2007). Finally, G2E systems face privacy and safety issues of providing employees with access to employee benefit information and communication portals with human resources departments (Pardhasaradhi & Ahmed, 2007).

Besides technical and structural risks, the historic development of many e-government information systems in a "vacuum" rather than through coordinated efforts have led to incompatibilities with other systems and data redundancy (i.e., the same data is stored in more than one place). These incompatibilities result in citizen and legislative outrage, as well as increased costs, poor performance, and a lack of sharable components and data (Park & Ram, 2004).

## **KNOWLEDGE MANAGEMENT AND RETRIEVAL IN E-GOVERNMENT**

Now that a discussion of technological and organizational challenges with government information systems faced by e-government in KM and retrieval has been presented, this section will discuss how the BSC can be used to ensure trusted e-government services and transactions.

Because uses within e-government environments vary widely (including even debt or courtroom trial management and litigation support), it is important to consider the skill-set and priority diversity of users, as well as organizational core

capabilities. Integrated e-government systems must be able to manage data/document capture, convert data to digital format, allow for Internet/intranet document publishing, track correspondence and electronic information distribution, and complete action tracking functions (such as suspenses and corrections) in a systematic manner.

The balanced scorecard, first introduced by Kaplan and Norton (1992, 1996a, 1996b), can be modified for e-government use to provide one of the best frameworks to enhance the integrated retrieval functions of KM systems. One of the key advantages of this approach is that it provides order to the unstructured nature of electronic data or text mining through a systematic process of extracting knowledge. Secondly, the BSC modification continues to support, improve, and add value to the productivity of data warehouse retrieval capabilities. Using four perspectives (finance, customers, internal processes and training growth), the BSC promotes continuous improvement at each phase of the KM process for e-government. As Figure 1 shows, each step of the KM strategy addresses these perspectives and continually transforms the review and audit function to evaluate knowledge created.

Basically, the finance perspective addresses timely and accurate funding data, as well as issues of risk assessment and cost-benefit data associated with the KM system (Arveson, 1998). The kinds of customers, processes used to service these groups, value-added service delivery, and satisfaction metrics are all part of the customer perspective (Davison, Wagner, & Ma, 2005). The internal business process perspective focuses on how well the organization is performing its mission mission-oriented processes (i.e., specific and unique functions of the e-government environment) and support processes (i.e., more repetitive functions benchmarked using generic metrics) (Patton, 2007). Finally, the training growth perspective highlights employee training and attitudes toward the organizational culture can lead to strengthened user communications for problem solving (Wu, 2007).

The knowledge audit is both the beginning and ending point that closes the loop when establishing effective e-government KM strategies. At a minimum, the knowledge audit should: (1) determine what target areas of knowledge should be audited and what limitations exist; (2) identify benchmarks and how results will be measured and tracked against this reference; and (3) evaluate existing/missing knowledge in target areas (Daghfous & Al-Nahas, 2006). After identifying the parameters of the knowledge audit, the strategic steps will of KM will examine perspectives of reducing costs (financial), enhancing customer value (customer), leveraging advantageous organizational processes (internal processes), and promoting change in the KM system through continuous learning cultures (training growth). Figure 2 displays examples of each perspective that could be incorporated when developing the organization's

5 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/chapter/knowledge-management-government/13912](http://www.igi-global.com/chapter/knowledge-management-government/13912)

## Related Content

---

### Security Implications for Management from the Onset of Information Terrorism

Ken Webb (2010). *Information Resources Management: Concepts, Methodologies, Tools and Applications* (pp. 2163-2183).

[www.irma-international.org/chapter/security-implications-management-onset-information/54592](http://www.irma-international.org/chapter/security-implications-management-onset-information/54592)

### Enabling Quality Assurance Analytics through the Use of Information Systems: The Case of a Juice Manufacturing Company

Au Voand Rahul Bhaskar (2014). *Journal of Cases on Information Technology* (pp. 1-13).

[www.irma-international.org/article/enabling-quality-assurance-analytics-through-the-use-of-information-systems/109513](http://www.irma-international.org/article/enabling-quality-assurance-analytics-through-the-use-of-information-systems/109513)

### Virtual Team Trust: Instrument Development and Validation in an IS Educational Environment

Saonee Sarker, Joseph S. Valacichand Suprateek Sarker (2003). *Information Resources Management Journal* (pp. 35-55).

[www.irma-international.org/article/virtual-team-trust/1239](http://www.irma-international.org/article/virtual-team-trust/1239)

### The Impact of the Mode of Data Representation for the Result Quality of the Detection and Filtering of Spam

Reda Mohamed Hamou, Abdelmalek Amineand Moulay Tahar (2017). *Ontologies and Big Data Considerations for Effective Intelligence* (pp. 150-168).

[www.irma-international.org/chapter/the-impact-of-the-mode-of-data-representation-for-the-result-quality-of-the-detection-and-filtering-of-spam/177392](http://www.irma-international.org/chapter/the-impact-of-the-mode-of-data-representation-for-the-result-quality-of-the-detection-and-filtering-of-spam/177392)

### Numbers and Symbols

(2013). *Dictionary of Information Science and Technology (2nd Edition)* (pp. 1-5).

[www.irma-international.org/chapter/numbers-symbols/76409](http://www.irma-international.org/chapter/numbers-symbols/76409)