

Survey: Enabled Embedding Innovation E Learning Bridging IT and E-Governance through ICT

Deepika Pathak ¹, Dr Sharad Gangele ²

¹Research Scholar, Department of Computer & Application, RKDF University Bhopal,
deepikapathak23@gmail.com

² Prof., Department of Computer & Application RKDF University Bhopal
sharadgangele@gmail.com

Abstract:

E-Governance can be an instrument of assurance of the administrative reform and modernization of public administration. A favorable environment for the transition to the Information Society will be created, which will correlate the interests of citizens, societal institutions, NGOs, private companies and the governance. It is evident from above discussion that objectives of achieving e-governance and transforming India goes far beyond mere computerization of stand alone back office operations. It means, to fundamentally change as to how the government operates, and this implies a new set of responsibilities for the executive and politicians. It will require basic change in work culture and goal orientation, and simultaneous change in the existing processes. Foremost of them is to create a culture of maintaining, processing and retrieving the information through an electronic system and use that information for decision making. It will require skilled navigation to ensure a smooth transition from old processes and manual operations to new automated services without hampering the existing services

I Introduction

Interactive Services Model Interactive-Service model is a consolidation of the earlier presented.

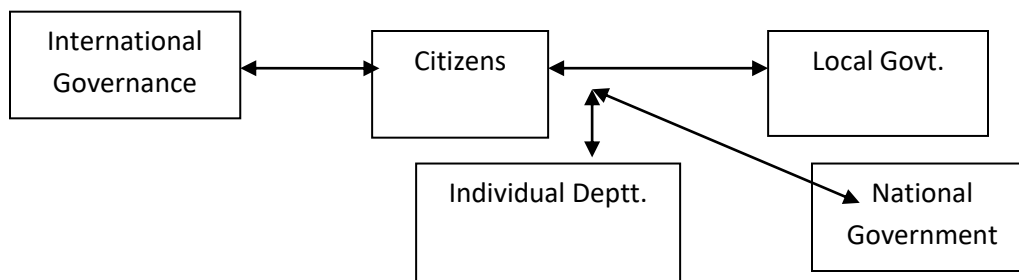


Figure 1.1

Digital governance models and opens up avenues for direct participation of individuals in the governance processes. Fundamentally, ICT have the potential to bring in every individual in a digital network and enable interactive (two-way) flow of information among them. The potential of ICT for the governance is fully leveraged in this model and leads and can bring lead to greater objectivity and transparency in decision-making processes.

To establish an interactive communication channels with key policy-makers and members of Planning Commissions. To conduct electronic ballots for the election of government officials and other office bearers. .

Philippine Customs Reform : Using an "off-the-shelf" customs application package as the main building block, the Philippines Customs Bureau has developed an on-line system to process clearance of imports, payment of duty, and delivery of release orders for shipments to leave the docks. The new on-line system has lessened the cost of trade for businesses, reduced opportunities for fraud, and helped the Bureau to maximize revenue collection.

Central Vigilance Committee (India) - pioneering initiative toward e-vigilance. It provides free-access information to citizens about government officials who have been indicted on judicial charges relating to corruption and have been advised penalty. People can also file complaints against any public servant who fall within the jurisdiction of the Commission.

The model firmly relies on the interactive applications of ICT and therefore is a technology and cost - intensive model which will require a transition period before being adopted on a wider scale, especially in the Developing Countries. It would also require elemental familiarity of ICT among the citizens to fully benefit from this model.

Organizations and Knowledge Networkers will have a tremendous role to play in widespread replication of this model.

II Comparatively Study Model:

Comparative Knowledge Model is one of the least-used but a highly significant model for developing country which is now gradually gaining acceptance. The model can be used for empowering people by matching cases of bad governance with those of good governance, and then analyzing the different aspects of bad governance and its impact on the people.

Essentially, the model continuously assimilates Best Practices in the areas of governance and then uses them as benchmark to evaluate other governance practices. It then uses the result to advocate positive changes or to influence 'public' opinion on these governance practices. The comparison could be made over a time scale to get a snapshot of the past and present situation or could be used to compare the effectiveness of an intervention by comparing two similar situations. The strength of this model lies in the infinite capacity

of digital networks to store varied information and retrieve and transmit it instantly across all geographical and hierarchal barriers. Public /private domain+ private/public /private domain=wider public domain

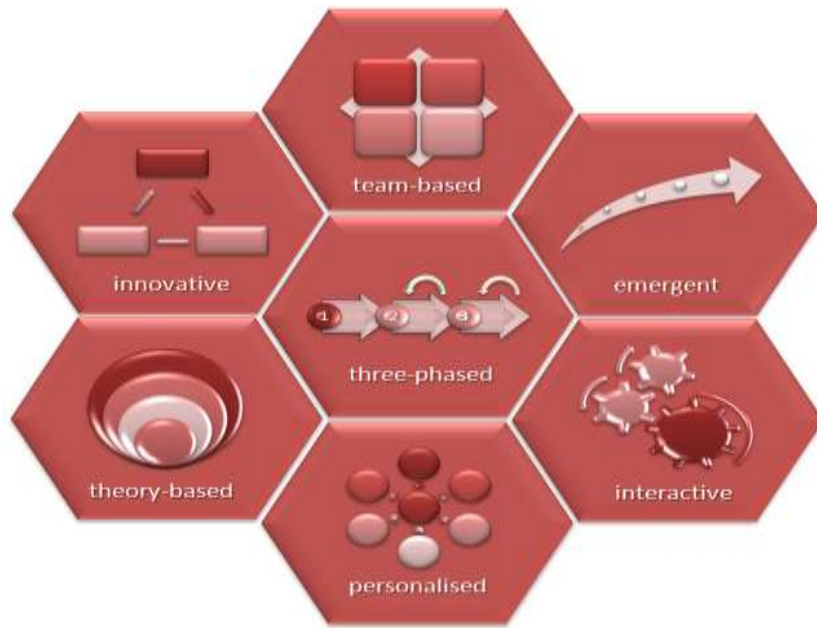


Figure 1.2

Theory-based: ensuring that decisions are based on contemporary approaches to teaching and learning.

Innovative: and relevant (incorporating elements of proactive evaluation documented by Sims, Dobbs & Hand, 2002).

Team-based: with team members having the relevant and appropriate competencies to engage with and complete the design tasks (Sims & Koszlaka, 2008).

Emergent: allowing (where appropriate) the interactions between course participants to establish and introduce course content (Irlbeck, Kays, Sims & Jones, 2006).

Interactive: enabling participants to actively explore the relevance and application of the course content (Allen, 2003; Sims, 2006).

Personalized: such that participants are able to apply their own context and situation to the learning outcomes (Sims & Stork, 2007).

As well as blurring the dividing line between private and public behavior in ICT, the electronic media are also big-challenging what we understand of what the notion 'privacy' is. Indeed, in a world where the media themselves appear to blur their own identities and purposes,ⁱ by allowing usersⁱⁱ to surf the internet on the television, watch films on their mobile and receive email on a fax machine, I believe we need to be especially aware of our 'core' identity, over and above the images we project of ourselves in both private and public settings. In this essay, I intend to further explore three

different electronic media, namely: mobile phones, the internet and television, by exploring current research and further 'real-life' examples, while also trying to take account of the partial amalgamation of media highlighted above.

In order to understand what we mean by 'private' and 'public' behavior as distinct social constructions, it is helpful to look at research into the social issues surrounding mobile telephony. This is because, unlike other electronic media, mobile phone conversations are highly interactive, i.e. they demand their users to craft immediate responses, regardless of their physical setting. Research into the behavior of new mobile phone users identifies the contrasting 'faces'ⁱⁱⁱ of people on the phone and off the phone as the main cause of people disapproving or even being offended by public mobile phone use. (Palen, Salzman & Youngs, 2000.) An example to explore how false our self-projected 'faces' are would be to consider behavior that could be adopted by a mobile phone user in an essentially artificial environment, such as a library. If someone on the phone in a library maintained the projection of themselves they adopted for that environment, anyone they were talking to would only hear a very quiet voice, if not a "shh..." or "be quiet!" This is entirely appropriate for the artificial hush of the library, but not for the contrasting environment of the phone conversation. Alternatively, the caller in the library could adopt a self-projection appropriate for the phone conversation; the result would be agitation from other library users. In this extreme contrast of location, it seems no compromise is possible, so the use of mobiles in libraries is seen to be socially inappropriate

On the internet, the question of being false is a much more prominent issue, indeed it is no longer a question but a reality. Individuals can actively exploit the methods of self-presentation to deceive people for malicious purposes and the media regularly make a point of informing the public of this. Deceptive or not, this medium is a powerful tool of 'personal construction;' of exploring, understanding, communicating and developing one's own personal identity. It is not always clear what 'face' we are presenting, and this perhaps makes the internet the stage for the most complex blurring of public and private behavior.

An example of a purely public self-presentation would be someone who projects a pseudonym i.e. someone who is not their self, but an entirely fictional character. Purposes for this behavior vary widely from experimental to, as mentioned above, malicious use. Contrasting this, a purely private self-presentation would be someone who is entirely genuine and truthful about how they present themselves, although this does increase vulnerability, and in practice could be argued as a more public self-presentation if it is consciously promoted in that way. This is however, becoming more and more common on personal websites, which individuals publish for family and friends although, technically, they are accessible to the wider public. Indeed, the significance of such sites has been described as 'one of the most dramatically visible signs of the construction of reality.' (Chandler, 1997) Although this brings up assumptions about reality itself: that it can be constructed or modified and hints at the possibility that maybe reality might not be real.

IV E-Governance life cycle

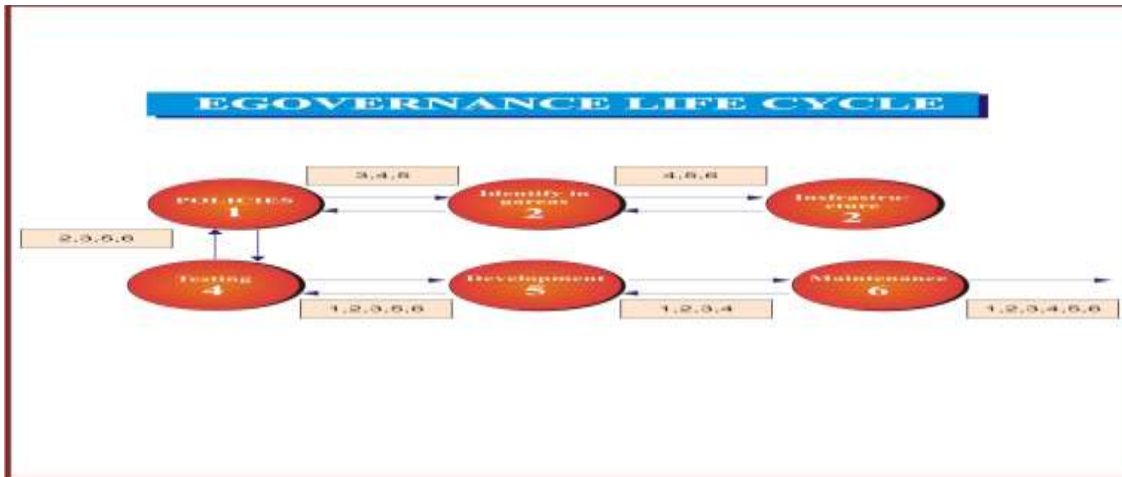


Figure 1.3

Governance and management of security are most effective when they are systemic, woven into the culture and fabric of organizational behaviors and actions. In this regard, culture is defined as the predominating shared attitudes, values, goals, behaviors, and practices that characterize the functioning of a group or organization. Culture thereby creates and sustains connections among principles, policies, processes, products, people, and performance. Effective security should be thought of as an attribute or characteristic of an organization or a project. It becomes evident when everyone proactively carries out their roles and responsibilities, creating a culture of security that displaces ignorance and apathy. One manifestation of this is that everyone proactively considers the attacker perspective throughout the software development life cycle and how the software can fail when under intentional attack or unintentional actions of users or developers.

This means that security must come off the technical sidelines as activities and responsibilities solely relegated to software development and IT departments. Today, boards of directors, senior executives, and managers all must work to establish and reinforce a relentless drive toward effective enterprise, information, system, and software security. If the responsibility for these is assigned to roles that lack the authority, accountability, and resources to implement and enforce them, the desired level of security will not be articulated, achieved, or sustained. Contrary to the popular belief that security is a technical issue, even the best efforts to buy secure software and build security into developed software and operational systems encounter "considerable resistance because the problem is mostly organizational and cultural, not technical" Software and information security are about spending money, with the measure of success being that nothing bad happens. As time goes on, this can become a tough sell to business leaders as the "we haven't been attacked lately so we can cut back on spending" mentality sets in.

Project managers need to elevate software security from a standalone technical concern to an enterprise issue when both developing and acquiring software. Because security is now a business problem, the organization must activate, coordinate, deploy, and direct many of its core resources and competencies to manage security risks in concert with the

entity's strategic goals, operational criteria, compliance requirements, and technical system architecture. Those responsible for ensuring secure software should have the responsibility and authority to stop the release of new software into production if security requirements are not met. To sustain enterprise security, the organization must move toward a security management process that is strategic, systematic, and repeatable, with efficient use of resources and effective, consistent achievement of goals.

V Conclusion:

(1) More effectively engage their leaders and executives in security governance and management by understanding how to place information and software security in a business context.

(2) Better understand how to enhance current management practices to produce more secure software. Armed with this material, managers and developers can build attentive, security-conscious leaders who are in a better position to make well-informed security investment decisions. With this support, they can then take actionable steps to implement effective security governance and management practices across the software and system development life cycle.

References:

- [1] Abbasi, Alireza, Niaraki, Abolghasem Sadeghi and dhko, Behzad Mirzaeian: "A review of ICT status and development strategy plan in Iran," International Journal of Education and Development, 2008, vol. 4, no. 3.
- [2] Bhattacharjee, D.S.: "Some Initiatives on ICT Enabled Teacher Education in India", ICDE International Conference, New Delhi, 2005..
- [3] Goyal, Ela, Purohit, Seema and Bhaga, Manju: "Study of satisfaction and usability of the internet on student's performance," International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2011, vol. 7, no. [6] Hung, Elias Said: "ICT use by Journalism Professors in COLOMBIA", Australian Journal of Educational Technology, 2011, vol. 27, no. 2.
- [4] Jaffer, Shaheeda, Ng'ambi, Dick and Czerniewicz, Laura: "The role of ICTs in higher education in South Africa: One strategy for addressing teaching and learning challenges", International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2007, vol. 3, no. 4. [8] Katherine, L. Dix: "DBRIEF: A research paradigm for ICT adoption", International Education Journal, 2007,
- [5] Krishnaveni, R. and Meenakumari, J.: "Usage of ICT for Information Administration in Higher education Institutions – A study", International Journal of Environmental Science and Development, 2010, vol. 1, no. 3.
- [6] Mehta, Deepa and Kasnia, Suman: "A Scenario on the role of ICT in Governance and Education System", IJCEM International Journal of Computational Engineering & Management, 2011, vol. 13. www.IJCEM.org .

[7] Mostert, Markus and Quinn, Lynn: "Using ICTs in teaching and learning: Reflections on professional development of academic staff," *International Journal of Education and Development using ICT*, 2009, vol. 5, no. 5.

[8] Oyel, N.D., Salleh, Mazleena and Iahad, N. A.: "Challenges of e-learning in Nigerian university education based on the experience of developed countries", *International Journal of Managing Information Technology (IJMIT)*, 2011, vol. 3, no. 2.

[9] Patel, Chirag J., Gali, Vidya S., Patel, Dhaval V. and Parmar, Ramesh D.: "The effects of information and communication technologies (ICTs) on higher education: From objectivism to social constructivism", *International Journal of Vocational and Technical Education*, 2011, vol. 3, no.5.

[10] Potashnik, M. and J. Capper: "Distance Education: Growth and Diversity", available from <http://www.worldbank.org/fandd/english/pdfs/0398/0110398.pdf> , accessed 2002.

[11] Qudais, Mahmoud Abu, Al-Adhlesh, Mosleh, and Al-Omen, Aieman: "Senior Faculty Members Attitudes in Jordanian Universities towards using Information and Communication Technology", *The International Arab Journal of Information Technology*, 2010, vol. 1, no. 4.

[12] Raji and Godsy: "ICT Use among Students of Arts and Science Colleges in Kerala", *Society for the Promotion of Alternative Computing and Employment Thiruvananthapuram*, March 2010.

[13] Sharma, Dharendra and Singh, Vikram: "ICT in Universities of the Western Himalayan Region in India: Status, Performance- An Assessment", *IJCSI International Journal of Computer Science Issues*, 2009, vol. 6, no. 2.