Association for Information Systems
AIS Electronic Library (AISeL)

GlobDev 2009

Proceedings Annual Workshop of the AIS Special Interest Group for ICT in Global Development

Winter 12-14-2009

Risk Management Decision Making in ICT for Development

Paul Rohmeyer
Stevens Institute of Technology, paul.rohmeyer@stevens.edu

Tal Ben Zvi
Stevens Institute of Technology, tal.benzvi@stevens.edu

Follow this and additional works at: http://aisel.aisnet.org/globdev2009

Recommended Citation
Rohmeyer, Paul and Ben Zvi, Tal, "Risk Management Decision Making in ICT for Development" (2009). *GlobDev 2009*. 4.
http://aisel.aisnet.org/globdev2009/4

This material is brought to you by the Proceedings Annual Workshop of the AIS Special Interest Group for ICT in Global Development at AIS Electronic Library (AISeL). It has been accepted for inclusion in GlobDev 2009 by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Risk Management Decision Making in ICT for Development

Paul Rohmeyer,
Howe School of Technology Management
Stevens Institute of Technology
paul.rohmeyer@stevens.edu

Tal Ben Zvi.
Howe School of Technology Management
Stevens Institute of Technology
tal.benzvi@stevens.edu

ABSTRACT

This paper explores the concept of enterprise resiliency in Information and Communications Technologies (ICT) for development initiatives. ICT are necessary to improve access to vital services and to ultimately support efforts to improve economic conditions in developing regions. Access to information resources provides substantial benefits in the public and private sectors of regions with low standards of living. Success in achieving any benefit from ICT investment in any development enterprise will be directly affected by the resiliency of the ICT systems and services, including technical and non-technical domains. We explore a framework to analyze risks and threats to enterprise resiliency, and present guidance to support the development of resilient ICT for development.

1. INTRODUCTION

What factors must be addressed to ensure that investment in Information and Communications Technologies (ICT) in developing regions produces high quality, reliable, and robust services and architectures? This basic question must be answered to achieve maximum return on global investment in ICT for development because implementation of a system that

lacks resiliency may prove disruptive to the target community or even undermine current and future development efforts.

The promise of ICT expansion in distressed regions can not be overstated. Basic elements of ICT have become expected and essentially mandatory resources in developed nations while many parts of the globe remain virtually isolated (Roberts 2008), (Avgerou 2008). There are many factors that have contributed to the current state, and therefore the lack of connectivity and computing resources is not surprising. As the use of ICT in virtually all facets of life in developed nations has continued to grow, the call to introduce the same information technologies into undeveloped regions has become increasingly urgent (Roberts 2008), (Boateng et al 2008). Today we are presented with the opportunity to make potentially historic and widespread improvements in the lives of millions by extending the reach of technologies such as broadband networking to drive access to healthcare, e-government, and education resources that would otherwise never reach those who arguably need them most.

Despite tremendous progress, the deployment of ICT for development has proven to be a significant challenge. This is due to factors such as high costs of technologies, regional shortages in a skilled labor pool to support deployment, poor physical security and in some cases armed conflict, and others An array of additional economic, political, and social challenges has contributed to the difficulties (Lindroos and Pinkhasov 2003), (Roberts 2008), (Wade 2002).

An important characteristic in the deployment of any information system is reliability. We maintain the value of ICT for development is determined by the nature and degree of support the ICT would provide to essential services demanded by society, and the value of such services would be diminished if the underlying ICT proved unreliable. Therefore there is a need for resilient ICT. Stated another way, maximizing resiliency in ICT will contribute to maximizing return on ICT investment as a reliable system that will meet expectations in delivering critical services more closely.

In this paper we examine the concept of resiliency from a broad perspective, one that extends beyond traditional technical viewpoints of redundancy, system backup or disaster recovery. Rather, resiliency in the fullest sense encompasses the need to design and build information systems to support critical processes and services. The information systems must be able to withstand an array of threats and either deflect or rebound from any risks events that become reality. However, it is not sufficient to address merely technical threats such as

cybersecurity or critical infrastructure risks. Resiliency therefore should be approached in a more comprehensive way that considers not only the technical but organizational and process domains as well, including areas such as strategy and culture. Deployment of robust ICT for development requires an ability to anticipate and understand the full range of factors that could lead to delay or disruption and to the engineering of robust solutions that can successfully face real challenges. It requires recognition that when ICT are deployed in developing regions to enable the delivery of vital services they may be severely handicapped by a variety of risks and ultimately provide little value in supporting broad development goals.

The remainder of the paper is organized as follows: in the next section we provide a literature review; then, we present analysis of threats to ICT for development. This is followed by a presentation and discussion of risk management guidance and our conclusions.

2. LITERATURE REVIEW

2.1. ICT for Global Development

ICT initiatives play a substantial role in global development. Cleverly (2009) predicted connectivity would generally become more prevalent and cloud computing would enable developing nations to gain rapid advances and perhaps "leapfrog" the developed world in some respects. He identified the potential for widely improved access to health care information and, potentially, services. In addition, the author stated that social networking would increase in richness and thereby enable members of developing nations to participate in all sorts of interactive pursuits; technology would be used against environmental and other resource challenges, and the advance of natural language technologies and other voice enabled systems would make Web resources easier to use.

Similarly, Paredes (2009) explored the promise and challenge of the implementing broadband networks in rural communities in the Dominican Republic to support national educational goals. The author observed ICT deployment first hand and recognized ICT as an important vehicle for the achievement of sustainable development in order to promote national improvements in efficiency and equity. A taxonomy of ICT projects in Tunisia is presented in Ouerghi (2007). ICT were a critical component of the e-Tunisia effort that sought to use information technologies to drive improvements in knowledge sharing, promoting competition,

promote education, and access to global markets. Pade (2006) noted that ICTs contribute significantly in supporting and promoting rural development and stressed the important role of knowledge sharing in rural development efforts, including the promise of participation in national, regional, and global communities. The author also suggested that the success of ICT projects could be diminished by a factors that affect deployment and usage.

Avgerou (2008) reviewed Information Systems research on intended benefits of ICT for development initiatives, including an examination of project failures. This included process, interaction, and expectation failures, respectively. Root causes were identified to include failures in technical scalability, sustainability of resources and political commitment, and dysfunctional process models failing to assimilate the ICT. Fuchs (2006) also described sustainability in the ICT development context, highlighting ecological, technological, economic, political, and cultural sustainability. Avgerou (2008) noted theories of the strategic importance of ICT in organizations have been extended to the development context. Boateng et al (2008) examined the diffusion of e-Commerce into development contexts and identified economic, socio-cultural, and legal impacts.

2.2. Enterprise Resiliency

Gaddum (2004) defined resiliency as *"The ability of an organization's business operations to rapidly adapt and respond to internal or external dynamic changes – opportunities, demands, disruptions or threats – and continue operations with limited impact to the business."* The author identified the merits of considering the concept of resiliency from organizational and business, and not strictly IT, perspectives, and presented a model of six layers of resiliency: strategy, organization, process, data and applications, technology, and facilities.

McManus (2007) described resilience as a function of an organization's situation awareness, management of key vulnerabilities, and its capacity to adapt in a complex, dynamic and interconnected environment, and described a resilience management process based on those factors. Oldfield (2008) noted there were numerous types of resilience, including corporate, business, enterprise, emotional, individual, organizational, sectoral or societal. Oldfield suggested an organization's resiliency was a factor of its adaptive capacities, communications, interdependencies, situational awareness, leadership, enterprise perspective, and culture. Bell

(2002) described the Resilient Virtual Organization (RVO) including domains of leadership, culture, people, systems, and settings.

Organizational rigidity was identified as a possible impediment to resilience in Denhardt (2009). The author suggested flexible organizations were naturally suited to adjust to developing threats and therefore might be better in responding to actual risk events as they unfold. Denhardt also suggested that a degree of excess capacity might be an important and contributing factor to resiliency as such capacity could be marshaled in a time of crisis. Hiebert (2006) explored resiliency in the workplace, noting resiliency varied among individuals and includes internal and external (contextual) drivers.

One important aspect of resiliency is the role of governance. Multi-level governance structures can provide the capacity to adapt to various changes and enable the organization to manage for resilience (Armitage 2006). FSF (2008) proposed a multidimensional approach to improving global financial resiliency in response to the collapse of credit markets. This included increased oversight of capital, liquidity, and risk management, and enhancements to transparency and responsiveness to risk. Starr (2003) drew a distinction between enterprise risk management (ERM) and enterprise resiliency, as the former tends to be emphasis rigidity and system hardening against vulnerabilities and the latter promotes a more comprehensive, flexible, and ultimately context-driven approach. ERM approaches often prioritize vulnerability management tactics while resiliency programs emphasize organizational speed and agility. van Opstal (2007) proposed federal homeland protection efforts should be extended to include economic resiliency as a national priority, and identified information systems resiliency as a critical factor in supporting enterprise and, ultimately, economic resiliency.

2.3. Competitive Differentiation

ICT initially deployed for basic development goals may provide local populations capabilities to provide goods and services to global markets. Resiliency has the potential to be a competitive differentiator under such circumstances. Starr (2003) analyzed a technology company that was able to weather a crisis while a competitor, affected by the same crisis, could not continue to operate. It is logical that developing nations seeking to gain access to various markets via ICT capabilities will establish an advantage over other emerging competitors who do not have comparatively capable infrastructure (e.g. ICT). However, investment in information

systems will simply create potential that can only be realized if the systems prove reliable (Madon 2005). Global competition brings with it the threat of replacement by any of a large number of alternative provider; therefore, resilient ICT would be not only advantageous but in some cases necessary in order to retain newfound global service arrangements that are based on continuous execution within negotiated service levels.

3. RISK AND THREAT FRAMEWORK FOR ICT FOR DEVELOPMENT

In this section we introduce a framework with respect to ICT development risks and threats. We later use this framework as the basis for our recommendations in subsequent sections.

Any uncertainty in the deployment or operation of a system can be characterized as risk. Risk can be decomposed into basic elements of threat, vulnerability, impact, and likelihood of occurrence. Risk can also be considered from technical and project perspectives. Today risk is generally increasing due to the challenges of globalization, technological complexity, increased technical and process interdependencies, and other factors (FSF 2008), (van Opstal 2007), (Rohmeyer and Stohr 2004).

All technologies present inherent technical risks. Such risks are the result of flaws, poor quality, misconfiguration, and/or incompatibilities that result in dysfunction. ICT initiatives are presented with project risks that threaten to diminish the value of the ICT investment. Project risks include any factors that impede successful deployment. Pade (2006) explained ICT project outcomes may be characterized as total failures, partial failures, or successes, with respect to attainment of major goals. The author claimed that further consideration must be given to sustainability or the capability the system to continue operating at full or partial success in order to provide an enduring benefit (i.e. resilience).

Gerhan and Mutala (2004) described extreme network bandwidth limitations at the University of Botswana and chronicled financial, political, and project challenges that are leading to a "quality" digital divide marked by basic connectivity but inferior service levels. Wade (2002) also noted the possibility of low quality service in newly connected nations. Lindroos and Pinkhasov (2003) chronicled risks inherent in the development context, focusing not only on access but quality of use. The authors noted "for the information society to take

hold, one very serious battle to win is to enhance trust and confidence in ICT and networked systems". The paper suggested the importance of building a "culture of security".

We define a threat as any factor that challenges any state of resiliency. In establishing a threat framework for ICT for development we first need to identify all pre and post conditions that represent potential disruptors to the project and, ultimately, the completed system. Any disruptor to people, process, and technology in the context of ICT deployment or operation should be considered. However, the variety of ICT types and deployment environments suggests splitting of the threat analysis into examination of general and application-specific risks, respectively.

We also need to consider threats of varying impact. In technical planning there is sometimes a tendency to consider catastrophic but theoretical threats at the expense of threats that are less novel and impactful, however more probable. Common threats to the organizational value chain, incidents that sometimes would not be reported outside of the organization, are nonetheless damaging the ability to deliver services. van Opstal (2007) similarly noted the evaluation of threats to resiliency should not be limited to catastrophic incidents.

Threats to successful deployment of ICT in developing regions are significant as reflected in the literature. In our framework we view threats in categories of financial, technical, deployment, environment, and process, which are visible across general domains of people, processes, and technologies.

Financial threats include a failure to obtain, or retain, adequate funding to support the initiative. ICT deployments can span months and years and therefore may not sustain the shifting sands of politics or turbulence in the greater economy, both of which threaten continued funding. Local providers of resources and skills are also subject to the same forces and may therefore be forced from business during a deployment.

Technical threats to development ICT initiatives include the same array of factors faced by information systems deployment in developed regions plus additional, especially challenging ones. This may be due to financial constraints or the lack of local providers and service organizations. There are sometimes no local technology providers or trustworthy shippers in the region of the project site, increasing costs and the likelihood of loss due to breakage during shipment, theft and corruption. The general availability of computing hardware may be similarly restrained in some areas, and it may prove not feasible to enforce any sort of hardware standards

due to the availability constraints. Software may be unavailable as well, requiring configuration teams to obtain their software electronically which in turn may be disrupted by limited or unpredictable network access services or a lack of reliable electricity service. Challenges such as these this can be overcome through a variety of means however the result is often increased cost, complexity, and longer project schedules. The string of technical interdependencies makes tasks that are otherwise simple in developed regions very challenging in ICT initiatives for development.

Once the ICT is operational it will be subject to the same threats of malicious code, system attacks, and eavesdropping faced by Internet systems the world over. However it will also be at the mercy of many local process and environmental control challenges. This includes but is not limited to theft (of money, data, or computing resources), misuse, vandalism, and terrorism as well as natural disasters. Areas experiencing any degree of armed conflict are presented with even more substantial difficulties.

The remaining category, threats to process, may be misunderstood or even overlooked in environments that have not experienced widespread deployment of information systems. Developed regions have experienced first hand that integration of ICT into any organization often results in improvements to productivity and therefore efficiency. However not as clear is the recognition of the threat of increased reliance on the new system, which increases the impact dimension of a risk event. Processes that were largely automated before, after having been transitioned into ICT, become dependent on the underlying ICT. Therefore a system disruption can quickly become a process, service, and perhaps organizational disruption. Organizations in developing regions that aspire to improve their fortunes by competing in the global services marketplace are particularly vulnerable because they are competing in a marketplace that includes providers that face substantially less risk.

4. MANAGING THE RISKS OF ICT FOR DEVELOPMENT

In this section we explore and synthesize the literature into our risk and threat framework. Our framework supports evaluation of the dimensions of enterprise and technical resiliency, and emphasizes the importance of culture, planning, enterprise risk management, alignment, design, and governance. Management of project and operational risks is essential to the success of

development initiatives. The following is a summary of the major themes and explanation of applicability to our framework.

4.1. Enterprise Resiliency

An important goal in deploying ICT for development is the creation of robust capabilities to support and promote a resilient enterprise. SEI Resiliency Management Model (2008) (RMM) and SEI Resiliency Engineering Framework (2008) (REF) provide substantial guidance on enterprise resiliency. RMM was architected to promote continuity in service delivery. ICT, but nature, are services, and also provide a platform to enable and support other services. RMM defines service continuity to include technical and process domains and recommends organizations develop plans to achieve resiliency based on their unique risk environment and other factors. RMM recommends organizations identify high-value services, assess the risks to those services, and calculate the consequences of risk events. REF is closely related to the CMM-I (SEI Capability Maturity Model for Integration) and promotes an enterprise perspective in the engineering of resilient information systems, including domains of enterprise management, engineering, operations, and process management. Enterprise resiliency therefore combines technical and non-technical domains.

4.2. Culture

It is vital to build a culture of resiliency to support ICT development and operations. The success of any implementation will be limited if the new system is not reliable. Weeks (2009) explained the importance of building a culture of resiliency awareness, and offered guidance on how to do so in Weeks and Benade (2009). McManus (2007) identified similar requirements. Deployment of any technology into developing regions presents significant challenges. Development ICT initiatives are faced with all of challenges faced by any technology deployment. However they also face unique dimensions of uncertainty related to factors such as cross-border and cross-cultural deployment, severe funding limitations, cumbersome governance processes of supporting agencies, corruption, and physical security. Therefore uncertainty in ICT deployment is much greater than in corporate ICT. This general increase in uncertainty should be expected to have profound impacts on many aspect of the project, including the

importance of quality, sustainability, and reliability in the new system. The challenges in building culture on projects and within the new support organizations that will maintain the new ICT are substantial however they must be addressed.

Similarly, McManus (2007) described a resilience management process that included identifying the need to build awareness of resilience issues, selecting organization-critical components, completion of a self-assessment of vulnerabilities, identification of key vulnerabilities, and what was characterized as increasing adaptive capacity, represented by a continuum that sought to move the organization away from functional silos to mature and integrated leadership, management, and governance structures. A high level mapping of strategic concerns was also provided in Pade (2006) that identified domains of sustainability in development initiatives as socio-cultural, institutional, economic, political, and technological. Heeks (2003) examined design-related failures in e-Government, while Wade (2002) identified the challenges of building and supporting multi-layer solutions that present inherent compatibility and management challenges in ICT for development.

Cultural challenges were similarly explored in Dalberg (2006) that observed cross-cultural ICT initiatives are faced with unique challenges and provided guidance on requirements and design activities to overcome cultural barriers. Xu (2008) stressed the need to employ case studies in the planning process in order to learn about historical disruptions and suggesting using the generalized risk elements of the respective cases to motivate the organization to recognize the need for resilience.

Kefallinos, Lambrou and Sykas (2009) presented an extended risk assessment model for secure e-government projects. The model incorporated fundamental risk dimensions of impact, probability, critical success factors, countermeasures, costs, and residual risk which the authors characterized as “coverage”. The model suggests the fundamental risk dimensions should be evaluated at various “levels” including political, regulatory, financial, procurement, and interoperability.

4.3. Technical Resiliency

Achieving technical resiliency is required to enable success in ICT development enterprises. Radhakrishnan (2008) presented a model of key performance indicators for IT Service management that may be directly applied to the ICT context. Radhakrishnan identified

the concept of "high availability service management"(HASM) to prioritize resiliency within the IT service management domain through the use of Six Sigma and other quality methods. HASM emphasizes system event and incident management as well as high quality infrastructure, architecture and design towards the objective of building sustainable systems.

Writing on the Resilient Economy, van Opstal (2007) examined the challenge of balancing competitiveness and security, and identified the need to adopt a resilience perspective that promotes agility and adaptability instead of static or compliance-driven security. Similarly, the Global Cybersecurity Agenda (GCA) was created by the International Telecommunication Union (ITU) with the support of various government and non-governmental groups, with focus on improving cybersecurity in the following domains (ITU, 2008): Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation. van Opstal (2007) and ITU (2008) both suggest improvements are needed to traditional technical protection models to support the new interdependent global services paradigm and presented strategic technical guidance.

4.4. Planning

ICT development efforts should be guided by formalized planning that takes proactive and reactive viewpoints with respect to risk management. Effective ICT should not simply follow the traditional definition of resilience (i.e. ability to rebound or bounce back from an incident) but to block the effects of incidents as well (i.e. repel). Weeks (2009) explained the importance of including both proactive and reactive postures in the resiliency model. Resilience in the broad sense suggests an ability to withstand events, system attacks, physical disruption, and other possible incidents. Organizations should adopt a comprehensive scope of planning. Pade (2006) identified domains of sustainability in development initiatives as socio-cultural, institutional, economic, political, and technological, and planning activities should take a similarly broad perspective. There is a substantial literature on risk assessment and technical planning to support operational and business continuity, which was summarized in Rohmeyer, Stohr (2004).

4.5. Design

Resiliency should be built into the enterprise design. It is imperative that ICT development teams promote concepts of robustness, stability, and high-availability at the earliest design stages. Technical, process, and information interdependencies should be considered. The organization that will rely on the operational ICT system should similarly be designed for resiliency, incorporating themes of awareness building and organizational redundancy as suggested by the literature. Development projects should include specific programs to protect revenue-generating processes through technical, process resiliency and organizational resiliency. Mbambo and Cronje (2002) chronicled World Wide Web utilization in small and medium sized businesses in Botswana and highlighted the importance of understanding localized information management needs. Osterwalder (2004) similarly examined ICT use of small and medium sized businesses in developing countries and presented business model guidance for ICT-based business models with the intent of integrating with the supply chains of developed nations.

4.6. Continuous Enterprise Risk Management

There is a need to continuously evaluate the unique risk elements of each organization and ICT initiative. An effective enterprise risk management (ERM) process would therefore be beneficial. Starr (2003) and McManus (2007) offered guidance on evaluating the organization as part of designing an ERM structure. Such an evaluation can be used to identify the unique risk elements. Starr (2003) presented steps to achieve resiliency as assessment of enterprise risk, use of the risk assessment as feedback to strategy and operations, and development of an organizational structure that uses available information to monitor risk and can respond as risk factors change. McManus (2007) also echoed the need to improve situational awareness so the organization can build a capacity to adapt to risk as challenges or risk dimensions change. All levels of risk should be considered within the model, from minimally disruptive through existential threats.

An output of the ERM process should be a resiliency management program (RMP). The RMP should include a controls architecture that presents a control point for each enumerated risk. The RMP should attempt to identify all threats to resiliency. Each threat should be analyzed in regards to the respective vulnerabilities, the impact of the risk event, and likelihood

of occurrence. Once these risk factors are considered, an appropriate mitigation strategy (i.e. control) should be designed for each threat. A method for monitoring and testing each control should be established as well as a schedule for period testing.

It is important to align the RMP with the strategic objectives and strategy of the ICT initiative and, perhaps, the development sponsor. The outcomes of the development effort should be important drivers in the RMP development process. RMP developers may therefore be best served by considering threats with respect to each ICT outcome and develop a risk matrix as shown in Table 1 and in the example that follows.

Table 1. Sample Resiliency Management Analysis for ICT for Development

	Outcome	Threat	Vulnerability	Impact	Likelihood	Mitigation	Monitoring
Generic Resiliency Management Analysis	The desired benefits of the development ICT	Potential disruptor	A weakness in a system.	The outcome of an actual disruption.	The probability of occurrence	Steps taken to reduce the impact of the disruption (i.e. a control)	Continuous validation of the operational effectiveness of the control.
Example	Provide access to healthcare information to medical professionals in remote locations.	Network connectivity is limited to one provider.	The service of the single provider may become unavailable.	Medical professionals may not be able to treat patients.	Determined by the robustness of single provider solution.	Identify an alternative connectivity path such as a backup provider or mini satellite dish.	Instruct users to gather and monitor network availability statistics.

The example of Table 1 demonstrates development ICT that are intended to provide information access for healthcare professionals. They should also identify a resiliency objective of uninterrupted connectivity at important healthcare centers and thus, address the basic risk elements described in the table.

The risk evaluation of an ICT for development project should similarly entail listing all desired outcomes of the development exercise accompanied by the analysis of corresponding risk to each objective as shown in Table 1. Ideally, this process should be initiated during the design stage of the initiative so feedback on significant risks can be considered by designers and architectures to help minimize inherent risk characteristics.

4.7. Governance

It is important to e*stablish pre- and post-implementation governance structures*. Governance considerations vary across the implementation lifecycle. The organizations and individuals involved in planning, design, and deployment in many cases will often not be involved in the ongoing operations of the ICT. Therefore it is import to identify governance structures that will oversee funding, internal controls, and reporting from pre and post perspectives.

Operational ICT should include structures to include accountability to maintain the Resiliency Management Program. The responsibility of local managers and technicians must extend beyond basic service provisioning and emphasize the importance of delivering high quality, reliable, and dependable service. Madon (2005) examined governance challenges in the deployment of call centers (telecentres) in Kerala and explored aspects of call center sustainability.

5. CONCLUSIONS AND POTENTIAL FUTURE RESEARCH

The importance of deploying ICT for development as a critical enabler of greater development goals in the support of development enterprises has been stressed throughout this paper. The desired outcomes however will be diminished or even made impossible if delivered systems (including technical and non-technical domains) prove unreliable in serving local objectives. Most importantly, resilient ICT are essential in building and sustaining resilient enterprises. The promotion of a culture of resiliency is therefore an urgent requirement to promote the continued success of ICT for development initiatives.

It is apparent development ICT initiatives routinely face significant challenges, difficulties that surpass the common hurdles of information systems deployment in the developed world. In development initiatives funding is often tightly constrained, local support may be minimal, and there may be significant infrastructure hurdles. There may also be a general lack of technical awareness and understanding at the local level or even regional level. In some cases the local population may simply not be supportive of the proposed ICT deployment despite the substantial benefits that planners and sponsors envision. Therefore, many of the steps suggested in this paper will simply prove unreasonable if not practically impossible in some project

settings. Nonetheless this paper presented a generalized model for a Risk Management Program for ICT for development that may contribute to project and operational success by establishing a resiliency goal and illustrating the genuine risks to system owners and operators. So while an exhaustive risk analysis and mitigation program may not be feasible in some cases, even partial implementation of a risk-oriented framework should be expected to provide benefits.

This paper was an initial step to introduce the goal of enterprise resiliency and the tactic of enterprise risk management in the arena of development ICT. We established a basis of relevant risk management guidance and identified barriers to success in broad terms. Future research in this area is needed to provide further guidance including a proposed implementation standard for ICT development efforts to promote enterprise and system resiliency.

REFERENCES

1. Armitage, D., 2006. "Resilience management or resilient management? A political ecology of adaptive, multi-level governance", I*ASCP 2006 Conference, Panel on Community-Based Conservation in a Multi-Level World*, Bali, Indonesia.
2. Avgerou, C., 2008. "Information systems in developing countries: a critical research review", *Journal of Information Technology 23*, 133–146, JIT Palgrave Macmillan Ltd.
3. Bell M. A., 2002. "The five principles of organizational resilience". *Gartner Research*.
4. Boateng, R., Heeks, R., Molla, A., Hinson, R., 2008. "E-commerce and socio-economic development: conceptualizing the link", *Internet Research*, Vol. 18 No. 5, 2008, pp. 562-594, Emerald Group Publishing Limited.
5. Cleverly, M., 2009. "Emerging Markets: How ICT Advances Might Help Developing Nations". *Communications of the ACM*, September 2009, Vol. 52, No. 9.
6. Dalberg, V., Angelvik, E., Elvekrok, D., and Fossbert, A., 2006. "Cross-Cultural Collaboration in ICT Procurement". *ACM GSD'06*, pp. 51-57.
7. Denhardt J. and Denhardt R., 2009. "Navigating the fiscal crisis: Tested strategies for local leaders". A White Paper from the Alliance for Innovation commissioned by the International City/County Management Association (ICMA).

8. Financial Stability Forum (FSF). 2008. Report of the Financial Stability Forum on enhancing market and institutional resilience.
9. Fitzsimmons, J.A & Fitzsimmons, M.J., 2008. *Services Management: Operations, strategy, information technology*, London: McGraw-Hill, 2008.
10. Fuchs, C., 2006. The implications of new information and communication technologies for sustainability", Springer Science and Business Media B.V. 2006.
11. Gaddum R., 2004. "Business resilience – the next step forward for business continuity". Available from http://www.continuitycentral.com/feature083.htm
12. Gerhan, D., Mutalam S., 2004. "Bandwidth Bottlenecks at the University of Botswana", *Library Hi Tech*, Vol. 23, No. 1, 2005. pp. 102-117. Emerald Group Publishing Ltd.
13. Heeks, R., 2003. "Most eGovernment-for-Development Projects Fail: How Can Risks be Reduced?", Institute for Development Policy and Management, University of Manchester, Harold Hankins Building, Precinct Centre, Manchester, M13 9GH, UK.
14. Hiebert, B. 2006; "Creating a resilient workplace," Division of applied psychology, University of Calgary. *NATCON Papers 2006 Les actes de la CONAT*.
15. International Telecommunication Union (ITU). 2008. *ITU Corporate Annual Report 2008*.
16. Kefallinos, D., Lambrou, M., Sykas, E., 2009. "An Extended Risk Assessment Model for Secure E-Government", *International Journal of Electronic Government Research*, Volume 5, Issue 2. IGI Global.
17. Lindroos, P., Pinkhasov, M., 2003. "*Information Society – The ICT Challenge*", The OECD Observer, Dec. 2003. Organization for Economic Cooperation and Development.
18. Madon, S., 2005. "Governance lessons from the experience of telecentres in Kerala", *European Journal of Information Systems (2005)* 14, pp.401–416, Operational Research Society Ltd.
19. Mbambo, B., Cronje, J., 2002. "The Internet as an information conduit in developing countries: an investigation of World Wide Web usability among small and medium textile enterprises in Botswana", *ASLib Proceedings*, Volume 54, Number 4, pp. 251-259.

20. McManus S., Seville E., Brunsdon D. and Vargo J. 2007. "Resilience management: A framework for assessing and improving the resilience of organisations", *Resilient Organisations Programme*: New Zealand, Resilient Organisations, Research Report 2007/01.
21. Oldfield R., 2008. "Organizational Resilience", *Continuity Forum News*, Vol. 11.
22. Osterwalder, A., 2004. "Understanding ICT-based business models in developing countries", *International Journal of Information Technology and Management*, Vol. 3, Nos. 2/3/4.
23. Ouerghi, M., 2007. "ICT Governance in Tunisia", *ACM ICEGOV2007*, Macao.
24. Pade, C., Mallinson, B., and Sewry, D., 2006. "An Exploration of the Categories Associated with ICT Project Sustainability in Rural Areas of Developing Countries: A Case Study of the Dwesa Project." *ACM Proceedings of SAICSIT*, pp. 100 –106.
25. Paredes, S., 2009. "The Social and Economic Impact from Broadband Implementation in Dajabón Dominican Republic." Masters Thesis, Stevens Institute of Technology.
26. Radhakrishnan, R., Mark, K., Powell, B., 2008. "IT Service Management for High Availability". *IBM Systems Journal*, Vol 47, No 4, pp. 549-561.
27. Software Engineering Institute (SEI), Carnegie Mellon University. 2008. "CERT Resiliency Engineering Framework Preview version, v0.95R" Available from www.cert.org/resiliency/
28. Software Engineering Institute (SEI), Carnegie Mellon University. 2008. "CERT Resiliency Management Model, v1.0, Service Continuity (SC)", Available from www.cert.org/resiliency/
29. Starr R., Newfrock J. and Delurey M., 2003. Enterprise resilience: managing risk in the networked economy. *Strategy + Business Magazine*, Vol. 30.
30. Roberts, S., 2008. "The Global Information Society: a Statistical View", A Publication by the *Partnership on Measuring ICT for Development*, Available from: http://measuring-ict.unctad.org/
31. Rohmeyer, P. and Stohr E., 2003. "An Examination of Business Continuity Planning Practices in the Pharmaceutical Industry". PhD Dissertation, Stevens Institute of Technology.

32. van Opstal, D., 2007. "The Resilient Economy: Integrating competitiveness and security", A publication by the *Council on competitiveness*. Available from http://www.compete.org/publications/idea/2/risk-and-resilience/

33. Wade, R., 2002. "Bridging the Digital Divide: New Route to Development or New Form of Dependency?", *Global Governance*, Vol. 8. pp. 443-466.

34. Weeks, R., 2009. "Resiliency Management within a Globally Integrated Economic Network", Accepted for publication in Acta Commercii.

35. Weeks, R. & Benade, S., 2009. "Nurturing A Culture Of Resiliency In The Age Of Fundamental Change". *Proceedings of the Portland International Center for Management of Engineering and Technology (PICMET) Conference*, Portland, OR.

36. Xu, J., 2008. "Managing the Risk of Supply Chain Disruption: Towards a Resilient Approach of Supply Chain Management". *2008 ISECS International Colloquium on Computing, Communication, Control, and Management*, Guangzhou City, China.