Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2010 Proceedings

Mediterranean Conference on Information Systems (MCIS)

9-2010

RISK MANAGEMENT DECISION MAKING IN SERVICE DESIGN

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

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

Follow this and additional works at: http://aisel.aisnet.org/mcis2010

Recommended Citation
Rohmeyer, Paul and Ben-Zvi, Tal, "RISK MANAGEMENT DECISION MAKING IN SERVICE DESIGN" (2010). *MCIS 2010 Proceedings*. 73.
http://aisel.aisnet.org/mcis2010/73

This material is brought to you by the Mediterranean Conference on Information Systems (MCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in MCIS 2010 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

RISK MANAGEMENT DECISION MAKING IN SERVICE DESIGN

Paul Rohmeyer, paul.rohmeyer@stevens.edu

Tal Ben-Zvi, tal.benzvi@stevens.edu

Stevens Institute of Technology, USA

Abstract

This paper explores the use of risk management techniques to promote the design of resilient services. Success in achieving any benefit from a new service will be directly affected by the resiliency of the supporting service architecture including technical and non-technical domains. The concept of resiliency in services and enterprises is examined. We present a framework to analyze risks and threats to service resiliency, and offer specific guidance to support the development of resilient services and service architectures.

The risk assessment framework was created by combining a model of service provider gaps that represent dimensions of service quality with a risk analysis model. The framework includes identification of threats and inhibitors to closing service provider gaps. We maintain that risk in services will remain if service provider gaps are not closed.

Service-based business models and economies will succeed only if we view service resiliency as a strategic imperative. Effective service design techniques should be adopted, therefore, to include identification and mapping of the provider gaps and creation of appropriate mitigation strategies. This is accomplished by application of service blueprinting techniques and subsequent analysis of the visible risks. The model that we present facilitates the identification of weaknesses or vulnerabilities in services as well as the impact and likelihood of risk events and enables the planning of remediation activities at the design stage.

Keywords: Service Management, Service Design, Risk Management, Decision Making.

1 INTRODUCTION

What factors must be addressed to produce high quality, reliable, and robust services and service architectures? This basic question must be answered because implementation of a service that lacks resiliency may prove disruptive to the target enterprise or customer base. Designers of services require methodologies to facilitate the identification of service and process risks in order to promote design decisions that account for risk characteristics. Organizations not only need to assess risk but to apply the output of risk analysis as a decision support resource in a variety of contexts. We refer to these activities as Risk Management Decision Making. This must be done continuously in many domains. In this paper we explore the application of risk assessment to decisions about the design of services.

An important characteristic in the deployment of any new system is reliability. We maintain the value of service systems and architectures is determined therefore by the nature and degree of support the new service would provide to essential enterprise activities, and the value of such services would be diminished if the underlying systems and architecture proved unreliable. Therefore there is a need for resiliency in service design. Stated another way, the promotion of resiliency in the design of a service will maximize return on investment for the new service by producing reliable offerings that will meet customer expectations.

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 reliable systems to support critical processes and services. The 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 should be approached in a more comprehensive way that considers not only the technical but organizational and process domains, including areas of strategy and culture. Deployment of robust enterprise service architectures requires an ability to anticipate and understand the full range of risk 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 new services are designed they must be created with consideration of a variety of risks otherwise they would ultimately provide little value in supporting broad enterprise goals.

The remainder of the paper is organized as follows: in the next section we provide a literature review to support the explanation of fundamental concepts; then, we present analysis of threats to service resiliency. This is followed by a presentation and discussion of risk management guidance in the context of services and our conclusions.

2 LITERATURE REVIEW

2.1 Services and Service Design

Lacy and Macfarlane (2007) described services as “a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. Services facilitate outcomes by enhancing the performance of associated tasks and reducing the costs of constraints. The result is an increase in the probability of desired outcomes.”

The service industry is viewed by the US government as one of important strategic value. Carey (2008) stated services accounted for over 80% of total US GDP were increasing as a percentage of GDP in economies around the globe. The US Department of Commerce website reported in May 2010: “Overall, the United States is the world's premier producer and exporter of services. As the

largest component of the U.S. economy, the services sector includes all economic activity other than agriculture, mining, and manufacturing. U.S. services exports more than doubled over the past ten years, rising from $117 billion in 1989 to $246 billion last year. The dominant role that services play throughout the U.S. economy translates into leadership in technology advancement, growth in skilled jobs, and global competitiveness. Foreign markets offer incredibly bright prospects for further export expansion and for creating new jobs by companies exporting U.S. services, and we have barely begun to tap these markets." The size and continuing expansion of the service economy is a trend that is sure to influence business planning in the coming years in profound ways.

Businesses and governments should therefore be concerned with the deployment of robust, high quality services to ensure the stability of the increasingly interconnected marketplace. The quality of services with respect to effectiveness in execution and delivery has been explored by Zeithaml and Bitner (2002) who created a "gaps model of service quality". The gaps model can be applied to explore various dimensions of service quality. The model essentially described the "customer gap" that is the difference between customer expectation and the customer's perceived realized value. Closing the customer gap can be accomplished by considering four types of "provider gaps". Provider Gap 1 occurs when the provider does not know what the customer expects. Provider Gap 2 is when we do not select the right service design and standards. Provider Gap 3 is not delivering up to service standards, and Provider Gap 4 is not matching performance to promises. Each of the provider gaps represents a degree of failure in service delivery. Provider Gaps 1 and 2 specifically are concerned with matters of planning and design.

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.

Services are sometimes provided by integrated "systems of systems" that are designed to promote the co-creation of value by otherwise distinct entities. The emergence of co-creation strategies was explored by Ramaswamy (2009). Ramaswamy explained how increased interdependency creates shared risks. The operational definition of "enterprise" should therefore be modified to apply to the extended enterprise of partners, providers, and others who somehow touch the integrated value chain.

2.3 Competitive Differentiation

Services initially deployed for basic enterprise goals may prove to support new or enhanced capabilities that may become competitive differentiators. Therefore such services have potential strategic value. 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 enterprises seeking to gain access to new customers or markets via new service offerings may establish an advantage over other emerging competitors who do not have comparatively robust service offerings. However, investment will simply create potential that can only be realized if the operational service proves reliable (Madon 2005). Global competition brings with it the threat of replacement by any of a large number of alternative service providers. Therefore, resiliency 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. Technical services may be particularly at risk of being replaced by a global competitor should resiliency be lacking due to the sometimes low transitional costs to replace service-oriented technologies.

3 RISK AND THREAT CHARACTERISTICS FOR SERVICES

In this section we explore service risks. We later use these concepts 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. New service initiatives are presented with project risks that threaten to diminish the value of the service design investment. Project risks include any factors that impede successful deployment. Pade (2006) explained 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).

We define a threat as any factor that challenges any state of resiliency. In establishing a threat framework for services we first need to identify all pre and post conditions that represent potential disruptors to the project and, ultimately, the completed service. Any disruptor to people, process, and technology in the context of service deployment or operation should be considered. However, the

variety of service 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 largely theoretical threats at the expense of threats that although less novel and impactful are 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. 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 deployment initiative or the continuous operation of the service. Service deployments can span months and years and therefore may not sustain the shifting sands of organizational politics or turbulence in the greater economy, both of which threaten continued funding. Providers of resources and skills are also subject to the same forces and may therefore be forced from business during a complex deployment.

The remaining category is threats to process. Enterprises may have a general grasp of fundamental risk and threat dimensions. 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 unautomated before, for example, become highly dependent on the underlying information systems. Therefore a system disruption can quickly become a process, service, and perhaps enterprise disruption.

4 A FRAMEWORK TO MANAGE RISKS IN SERVICES AT THE DESIGN STAGE

In this section we explore and synthesize the literature into our risk and threat framework. Our framework supports evaluation of dimensions of service, enterprise, and technical resiliency, and emphasizes the importance of culture, planning, enterprise risk management, alignment, design, and governance in moving towards building service resiliency that is characterized by a minimized provider gap. Management of both the implementation and the operational risks is therefore essential to the success of service design initiatives. The following is a summary of the major themes and explanation of applicability to our framework.

As illustrated in Figure 1, the user of the service, the customer, only interacts with the service provider enterprise via service interactions. The service design acts as an abstraction layer, blocking the underlying organizational attributes from view. Thus the customer only assesses service quality on the basis of the provider gap. The service is moved closer to the customer's expectations (provider gap is reduced) by the support of adequately designed service architecture. The service architecture, as well as the service, are first designed to minimize the provider gap and subsequently subjected to continuous enterprise risk management. Therefore risk management is important in both the service design and the operational phases of deployment.

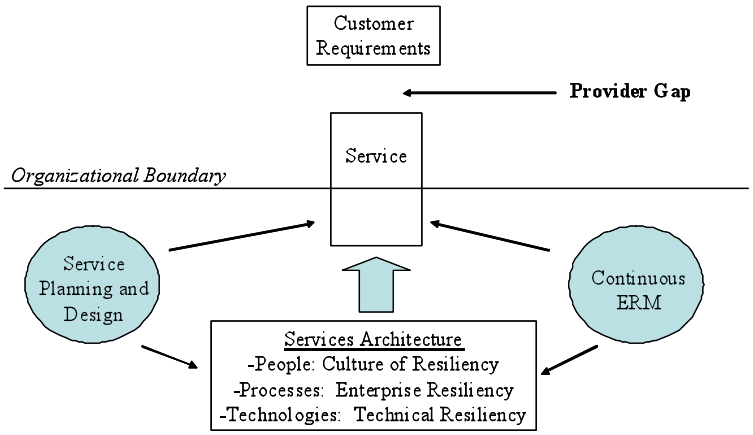

Figure 1. Conceptual Model of Risk Management in Service Design

4.1 Services Architecture: Creating a Culture of Resiliency

It is vital to build a culture of resiliency to support service design 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. 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.

Cultural challenges were similarly explored in Dalberg (2006) that observed cross-cultural 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.

4.2 Services Architecture: Enterprise Resiliency

An important goal in deploying new services 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. 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.

4.3 Services Architecture: Technical Resiliency

Achieving technical resiliency is required to enable success in new service enterprises. Radhakrishnan (2008) presented a model of key performance indicators for IT Service management. 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. US Senate (2009) introduced bill S.773 Cybersecurity Act of 2009, described as "a bill to ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes."

4.4 Service Planning and Design

New service design efforts should be guided by formalized planning that takes proactive and reactive viewpoints with respect to risk management. Resiliency should be built into the enterprise design. Effective services 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).

It is imperative that design 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 service 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. Osterwalder (2004) similarly examined small and medium sized businesses in developing countries and presented

business model guidance for information systems based business models with the intent of integrating with the supply chains of developed nations.

Carey (2008) described the technique of "service blueprinting" that may be useful in the service planning and design stages. Carey identified five components to be considered when analyzing the provider-customer interaction. "Customer actions include all of the steps customers take when using a particular service as part of the service delivery process. Onstage/visible contact employee actions are the actions of frontline contact employees that occur as part of a face-to-face encounter with customers. Backstage/visible contact employee actions are non-visible interactions with customers, such as telephone calls, as well as other activities employees undertake in order to prepare to serve customers or that are part of their role responsibilities. Support processes are all activities carried out by individuals in a company who are not contact employees, but whose functions are crucial to the carrying out of services processes. Physical evidence represents all of the tangibles that customers are exposed or collect to during their contact with a company." The structure for blueprinting described by Carey can provide the analysis framework a detailed evaluation of services in support of risk management activities.

4.5 Continuous Enterprise Risk Management

There is a need to continuously evaluate the unique risk elements of each organization and service 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.

The key input to the ERM process is a detailed service description. Blueprinting as described by Carey (2008), and explained earlier in this document, should be performed first to establish an understanding of the service flow as well as identification the systems and information components the service is based on.

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 initiative and, perhaps, the development sponsor. The outcomes of the development effort should be important drivers in the RMP development process.

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. Therefore it is import to identify governance structures that will oversee funding, internal controls, and reporting from pre and post perspectives. Operational services 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 and explored aspects of call center sustainability.

4.6 Risk Analysis Framework

As described the provider gap model characterizes various types and degrees of service failure and is therefore a sound base to build the risk assessment on. A general framework for evaluating service risks is presented in Table 1.

Outcome	Threat	Vulnerability	Impact	Likelihood	Mitigation	Monitoring
The desired value/benefits of the service.	Potential disruptor or inhibitor.	A weakness in any part of the service system or value-chain.	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.

Table 1. General Risk Management Framework

The risk evaluation for a particular service 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.

As explained previously, however, service risks are somewhat unique and therefore application of the gaps model would improve the analysis of service-related risks. A basic adaptation of the gaps model to the risk context is therefore presented in Table 2.

Provider Gap	General Threat(s)	Vulnerability	Impact	Likelihood	Mitigation	Monitoring
1 – Not knowing what customers expect	Insufficient data and/or analysis.	Poor market research or customer relationship management.	Creation of services that customers do not want.	Dependent on degree of innovation in the service.	Use of multiple approaches to assessing demand.	Know your customer.
2 – Not selecting the right service designs and standards	Ineffective decision making.	Poor design, Lack of customer-accepted standards.	Understanding demand but creating services that do not address it.	Dependent on degree of effectiveness in decision making.	Improve decision support and decision making processes.	Evaluate decisions via post implementation techniques.
3 - Not delivering to service standards	Operational failures, personnel challenges, poor forecasting of supply and demand.	Service design weaknesses, Inability to monitor partners, inadequate governance.	Understand demand, design the right service, but do not execute in operations.	Dependent on the ability of service providers to execute.	Vetting of employees and partners. Testing of architectures.	Monitoring programs for architectures, vendors, and personnel.
4- Not matching performance to promises	Failure to manage customer expectations.	Poor communication, Inadequate investment in customer relationship.	Customer interests, desires, requirements go unmet.	Dependent on effectiveness of the customer relationship management process.	Investment in customer relationship management.	Continuous evaluation of customer relationship personnel.

Table 2. Service Risk Analysis Framework Using the Gaps Model

Table 2 illustrates that risk management in the services context can be facilitated by devising tactics and strategies to overcome or avoid the inhibitors to closing the provider gaps.

5 CONCLUSIONS AND POTENTIAL FUTURE RESEARCH

Resilient services are essential in building and sustaining resilient enterprises. The promotion of a culture of resiliency is therefore an urgent requirement. This paper presented a generalized model for a Risk Management Program for service design that may contribute to project and operational success by establishing a resiliency goal and illustrating the genuine risks to system owners and operators. 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 via improved service resiliency.

As described in the paper we recommend the design of new services should include the use of (a) service blueprinting techniques to specify service characteristics in detail, and (b) service risk analysis techniques based on the provider gap model. This paper was an initial step to adapt the goal of enterprise resiliency to the services context. We established a basis of relevant risk management guidance and identified barriers to success in broad terms.

A next step in our research will be testing the model by completing risk assessments of a sample of implemented services. The assessments will seek to identify unmitigated risks and, if possible, isolate risks that could have been identified in the service design stage. A potential benefit of using the model is the early detection of service risks and therefore avoidance of a provider gap.

Future research in this area is also needed to provide additional techniques to improve service quality in order to support the enumeration and analysis of risks in systems characterized by heavy reliance on models of co-created value to promote the design of more resilient integrated services and service architectures.

References

Armitage, D., 2006. "Resilience management or resilient management? A political ecology of adaptive, multi-level governance", IASCP 2006 Conference, Panel on Community-Based Conservation in a Multi-Level World, Bali, Indonesia.

Bell M. A., 2002. "The five principles of organizational resilience". Gartner Research.

Carey, W.P., 2008. "A Key to Service Innovation: Services Blueprinting". Available from http://knowledge.wpcarey.asu.edu/article.cfm?articleid=1546%5C

Dalberg, V., Angelvik, E., Elvekrok, D., and Fossbert, A., 2006. "Cross-Cultural Collaboration in ICT Procurement". ACM GSD'06, pp. 51-57.

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).

Financial Stability Forum (FSF). 2008. Report of the Financial Stability Forum on enhancing market and institutional resilience.

Fitzsimmons, J.A & Fitzsimmons, M.J., 2008. Services Management: Operations, strategy, information technology, London: McGraw-Hill, 2008.

Gaddum R., 2004. "Business resilience – the next step forward for business continuity". Available from http://www.continuitycentral.com/feature083.htm

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.

Hiebert, B. 2006; "Creating a resilient workplace," Division of applied psychology, University of Calgary. NATCON Papers 2006 Les actes de la CONAT.

International Telecommunication Union (ITU). 2008. ITU Corporate Annual Report 2008.

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.

Lacy, S., Macfarlane, I., 2007. "Service Transition". The Stationery Office; 1 edition.

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.

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.

Oldfield, R., 2008. "Organizational Resilience", Continuity Forum News, Vol. 11.

Osterwalder, A., 2004. "Understanding ICT-based business models in developing countries", International Journal of Information Technology and Management, Vol. 3, Nos. 2/3/4.

Radhakrishnan, R., Mark, K., Powell, B., 2008. "IT Service Management for High Availability". IBM Systems Journal, Vol 47, No 4, pp. 549-561.

Ramaswamy, V. 2009. "Are You Ready for the Co-Creation Movement?", IESE Insight. Third Quarter 2009. Issue 2.

Software Engineering Institute (SEI), Carnegie Mellon University. 2008. "CERT Resiliency Engineering Framework Preview version, v0.95R" Available from www.cert.org/resiliency/

Software Engineering Institute (SEI), Carnegie Mellon University. 2008. "CERT Resiliency Management Model, v1.0, Service Continuity (SC)", Available from www.cert.org/resiliency/

Starr R., Newfrock J. and Delurey M., 2003. Enterprise resilience: managing risk in the networked economy. Strategy + Business Magazine, Vol. 30.

Rohmeyer, P. and Stohr E., 2003. "An Examination of Business Continuity Planning Practices in the Pharmaceutical Industry". PhD Dissertation, Stevens Institute of Technology.

US Dept of Commerce, 2010. Services Markets of Opportunity, U.S. Department of Commerce International Trade Administration. Available from http://www.ita.doc.gov/td/sif/services_markets.htm

US Senate. 2009. S.773 - Cybersecurity Act of 2009. Available from http://www.opencongress.org/

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/

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

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.

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.