Risk Management Considerations in Cloud Computing Adoption

Abstract

Information and Communication Technology (ICT) plays a pivotal role in enabling organizational capability and productivity, and in initiating and facilitating innovation across all industry sectors. In recent years, cloud computing has emerged as a growing trend because it serves as an enabler of scalable, flexible and powerful computing. Consequently, each year significant global investment is made in migrating to the cloud environment. However, despite its growing popularity, several risks and security concerns surround the cloud computing model. Therefore, understanding an organization's readiness and ability to mitigate associated risks is critical prior to embarking on the cloud computing journey. One approach to determining an organization's ability to effectively migrate to the cloud is to determine the current maturity of both its cloud computing capabilities and its risk management capabilities. As such, the Cloud Computing tool and the Risk Management (RM) Critical Capability of the IT Capability Maturity Framework (IT-CMF) are proposed as effective maturity assessment instruments to enable organizations to establish future roadmaps that will improve their maturity with respect to their cloud computing readiness. Increasing the level of maturity improves organizational practices surrounding the identification and mitigation of risks/threats that pertain to the cloud environment.

KEYWORDS: IT-CMF, cloud computing, risk management, risk mitigation, cloud adoption

Introduction

The National Institute of Standards and Technology (NIST) defines cloud computing as:

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

(NIST, 2011)

This cloud model promotes availability and is composed of five essential characteristics:

- On-demand self-service.
- Broad network access.
- Shared resources.
- Rapid provisioning.
- Minimal intervention.

Furthermore, it encompasses a variety of different service delivery models including *Infrastructure as a Service*, *Platform as a Service*, and *Software as a Service*, each of which has its own associated benefits and risks. These service delivery models are

supported by four primary cloud deployment models; namely, the *private*, *public*, *community* and *hybrid* cloud infrastructures. This model of computing resource delivery is regarded by many as an enabler of scalable, flexible and powerful computing, and consequently it has been more widely adopted in recent years.

Organizational Benefits from Cloud Computing Adoption

Cloud computing is increasingly asserted as the technology with the potential to change how the Internet and information systems are currently being used. It is deemed important in the area of IT innovation and it is increasingly recognized as being worthy of investment. More specifically, *cloud computing* facilitates data transactions along value chain activities such as manufacturing, finance, distribution, sales, customer service, information sharing and collaboration with trading partners. In some sectors such as the knowledge intensive high-tech sector, *always available* data transformation practices (inherent in the cloud) are perceived as key to improving operational efficiency. The cloud is also viewed as an effective mechanism through which organizations can enhance their competitive advantage by modifying how they buy, sell, and engage with their customers while becoming an integral element of the enterprises' overall business strategy.

Risk Management Considerations for Cloud Computing

Despite its growing popularity, several risks and security concerns surround the cloud computing model. A number of these cloud-specific risks are outlined in Table 1.

Table 1: Risks of Cloud Computing Adoption

Risk Area	Description
Security	Physical and personnel security: Access to physical machines and customer data may not be adequately controlled.
	Identify Management: Access to information and computing resources may not be controlled.
	Application Security: The applications that are available as a service via the cloud may not be secure.
	Data Confidentiality: There may be indirect control of data leakage prevention and latent problems with security in a multi-tenant architecture.
Lack of Standards	Data protection: There may be concerns over differences between international laws and regulations; for example, with respect to data protection.
	Open architecture: There is no standard open architecture defined for the cloud. Each of the major cloud providers (Amazon Web Services, Salesforce's force.com, Google App Engine, and Microsoft Azure) impose architectures that are different from both one another and from the common architectures currently used for enterprise applications.
Vendor/Data Lock-in	There may be concern over vendor or data lock-in due to contractual constraints and/or the cost to change vendor. Vendors use unique and proprietary user interfaces, application programming interfaces (APIs) and databases.
Software Licensing	Many licenses for packaged application software still impose restrictions on the physical machines on which the software can run.
Enterprise Level: support, service maturity, functionality	Cloud computing services may not provide the levels of reliability, manageability, and support required by large enterprises. Today, many cloud computing services are aimed primarily at Small and Medium Enterprises (SMEs) and at consumers, rather than at large enterprises.
Return on Investment (Rol)	The expectation is that external cloud computing can reduce costs for large enterprises as well as SMEs. However, the cost advantages for large enterprises may not be as clear as for SMEs, because many large enterprises can reap the benefits of significant economies of scale in their own internal IT operations, or because there is a lack of clarity on current IT consumption.
Connectivity	There is concern over connectivity and availability of an Internet connection because cloud computing is impossible without a reliable Internet connection. A dead Internet connection means no work, and in areas where Internet connections are few or are inherently unreliable, this could be a problem.
Compliance	How to ensure conformance to local, regional and global, statutory and legal requirements.
Trust and Viability of Service Providers	How to assess the viability and trustworthiness of the cloud service providers. Trust in the external provider to control and protect critical business data.
Computing Performance	Latency and programming scalability – concerns over latency or scalability in programming associated with the adoption of cloud computing.
Availability / Business Continuity	Concern over the continuous availability and the potential for downtime from the cloud service provider or from the Internet.

Maturing Organizational Readiness for Cloud Adoption

Improving organizational readiness for *cloud* adoption requires a structured and systematic approach; IT-CMF is an innovative and systematic framework that enables CIOs/CEOs to understand and improve their organization's maturity and consequently enable optimal business value realization from IT investments. IT-CMF represents an emerging blueprint of key IT capabilities and acts as an assessment tool and a management system, complete with improvement maps that help organizations to continually improve their IT capability over five levels of maturity – initial, basic, intermediate, advanced, and optimizing. At a macro level, IT-CMF consists of four integrated IT management strategies (macro capabilities) that underpin value-oriented IT management: managing IT like a business, managing the IT budget, managing the IT capability, and managing IT for business value. These four macro capabilities comprise 33 critical capabilities (CCs) that collectively represent key activities of the IT organization in delivering IT solutions and optimizing the associated business value generated. Each CC encompasses a number of categories and capability building blocks (CBBs) that reflect the CC's content and assumptions associated with each of the five maturity levels. Understanding an organization's current and desired maturity levels helps set improvement initiatives that drive value delivery over time. Improving maturity across the CCs reflects organizational progress, while metrics help determine performance effectiveness and value creation.

A particular area of developmental focus of the IT-CMF framework involves a cloud computing maturity assessment tool, which enables organizations to systematically determine their key strengths and weaknesses in migrating to the *cloud*. This tool supports not just an understanding of the organization's current readiness and desired maturity, but also helps define specific practices for the transition to higher maturity levels. The *IT-CMF cloud computing assessment* is developed using a cluster of IT-CMF's Critical Capabilities and focuses on the life cycle from cloud adoption readiness to the ongoing management of the cloud environment. The assessment is focused on nine capability building blocks across four categories, as outlined in Table 2. The assessment enables organizations to understand their level of maturity with respect to:

- Establishing their key goals and expectations from cloud adoption.
- Assessing appropriate business areas to outsource to the cloud and the impact of so doing.

- Defining strategies for the rollout of cloud services, including strategies for risk assessment.
- Detailing the new service, how it will be managed, how it interfaces to the existing/remaining systems, and how it will be monitored and reported.
- Selecting and contracting a suitable supplier based on value, sustainability and quality.
- Establishing a project team for transition to the cloud environment.
- Managing the cloud supply chain.
- Continually monitoring and reviewing the organization's cloud service requirements.

A review of each of these areas provides varying degrees of insight into an organization's maturity in addressing the obstacles/risks associated with cloud adoption. The IT-CMF cloud computing assessment provides organizations with a high-level understanding of their maturity in:

- Applying well-defined policies and governance frameworks to identify, assess and mitigate cloud-related risks.
- Developing a risk management process to mitigate the impacts of cloud migration on *all* staff (both IT and the business) during rollout of cloud adoption.

Due to the fundamental importance of effective management of risks/threats, based on the results from the IT-CMF cloud computing assessment, an organization may consider it is beneficial to gain a more in-depth insight into its risk management practices prior to the cloud "go/no go" decision. In such cases, the high-level cloud assessment could be supplemented by a detailed IT-CMF Risk Management assessment. The key categories and capability building blocks inherent in both assessments are outlined in Table 2 and Table 3:

Table 2: Cloud Computing Assessment

Category	Capability Building Block
Architecture (Cloud Proposition)	Investigate
	Identify
	Implementation Strategy
	Business Design
Engage	Selection
	Negotiation and Sign-Off
Operate	Operational Roll-Out
	Management of the Cloud supply Chain
Regenerate	Review

Table 3: Risk Management Assessment

Category	Capability Building Block
Governance	Policies for Risk Management
	Integration
	Management, Governance, and Performance Management
	Communication and Training
Profiling and Coverage	Definition of Risk Profiles
	Risk Coverage
Process	Assessment
	Prioritization
	Handling
	Monitoring

The Risk Management Critical Capability (CC) focuses on proactively assessing, prioritizing, handling and monitoring risks in order to minimize exposure and the potential impact of IT risk levels. Comprising nine capability building blocks, the IT-CMF Risk Management (RM) assessment provides key insights into an organization's maturity with respect to governance, risk profiling and coverage, and the actual risk management process, including:

- Defining and implementing risk policies, and establishing policy ownership and responsibilities.
- Integrating RM into IT leadership and governance structures, including decision-making processes and programme life cycles.
- Identifying RM roles and responsibilities.
- Measuring the effectiveness and efficiency of RM activities.
- Training stakeholders in RM and disseminating RM policies, processes and results enterprise-wide.
- Defining risk and threat profiles by their potential impact.
- Identifying and scoring risks and their impact.
- Prioritizing risks and risk-handling strategies.
- Defining and implementing appropriate risk controls.
- Tracking identified risks over time and the effectiveness of risk controls.

As such, the IT-CMF RM assessment represents the basis for the organization to understand key strengths and weaknesses in its ability to mitigate potential risks, including those pertaining to the cloud environment.

Concluding Remarks

In summary, the output from the IT-CMF cloud computing and risk management assessments enables an organization to develop roadmaps and to put action plans in place in order to mature its capability in effectively managing the risks/threats associated with cloud computing adoption. With a mature capability:

- Risk Management is planned, tracked, and monitored at the project, programme, and organization levels; lessons learned and feedback from Risk Management are incorporated.
- Risk Management is built into all relevant processes within the organization and IT Risk Management is integrated into Enterprise Risk Management (ERM) processes.
- Budgets are allocated effectively and efficiently, and there is a clear investment for risk mitigation.
- Risk Management is actively involved in controls assessment, controls design, and controls validation to ensure that it has more than just a consultant's role.
- Key IT risks are known, their business impact is quantified, and appropriate risk handling strategies are in place.
- Risk Management efficiency and effectiveness are confirmed at regular intervals.

Through maturing the organization's IT risk management practices, CEOs and CIOs can reduce the organization's exposure to risks associated with cloud computing adoption, and improve its ability to manage risks and protect the business from risk impacts. Further, they can benefit from an important interface that maps IT risks to the corresponding business objective. Through maturing RM practices and ability to effectively mitigate the risks associated with cloud adoption, an organization's readiness to effectively leverage the benefits of the cloud environment is increased. Over time, the organization can improve its cloud computing practices, facilitated by the actions identified through the IT-CMF cloud computing assessment, and by so doing it can mature its cloud computing capability. With a mature cloud computing capability:

- Cloud services are used, as and when required by the business in order to provide a flexible, highly responsive portfolio of integrated services to satisfy business requirements.
- Service providers become valued partners and there is transparency on security practices and compliance standards.
- IT is more responsive to business change and can scale/provision resources quickly.
- There is multi-platform and multi-Service Level Agreement (SLA) support.
- There is increased integration of social media and application stores.
- There is greater ease of on-boarding/ off-boarding.

References

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2010). "A view of cloud computing", *Communications of the ACM*, Vol. 53, pp. 50–8.

2. Curley, M. (2004). "Managing information Technology for business value – practical strategies for IT and business managers", *Intel Press*.

3. Curley, M. (2007)." Introducing an IT Capability Maturity Framework", *International Conference on Enterprise Information Systems*.

4. Gartner (2009). "Cloud computing inquiries at Gartner", available at: http://blogs.gartner.com/ thomas_bittman/2009/10/29/cloud-computing-inquiries-at-gartner *(accessed 16 January 2012)*.

5. Goscinski, A. and Brock, M. (2010). "Toward dynamic and attribute based publication, discovery and selection for cloud computing", *Future Generation Computer Systems*, Vol. 26, pp. 947–70.

6. Jackson, K. L. (2011). Forbes: "The Economic Benefit of Cloud Computing". Available at: http://www.forbes.com/sites/kevinjackson/2011/09/17/the-economic-benefit-of-cloud-computing/

7. Kundra, V. (2011). "Federal cloud computing Strategy". Available at: http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf *(accessed 12 June 2012)*.

8. Kynetix Technology Group (2009). "Cloud computing – A Strategy Guide for Board Level Executives". Available at: Microsoft Downloads. *(Accessed 12 June 2012)*.

9. Lo, C., Chen, Y., Wu, M. (2011). "Understanding the determinants of cloud computing adoption", *Industrial Management & Data Systems*, Vol. 111 No. 7, pp. 1006–1023.

10. National Institute of Standards and Technology (NIST) (2011) Final Version of NIST Cloud Computing Definition Published, online at http://www.nist.gov/itl/csd/cloud-102511.cfm accessed 27th August 2012.

11. Pyke, J. (2009). "Now is the time to take the cloud seriously", White Paper, at: www.cordys.com/ cordyscms_sites/objects/bb1a0bd7f47b1c91ddf36ba7db88241d/time_to_take_the_cloud_seroiusly_online_1_.pdf.

12. Thibodeau, P. (2010) "Frustrations with cloud computing mount", *ComputerWorld*, April, Available at: http://www.computerworld.com/s/article/9175102/Frustrations_with_cloud_computing_mount

About the Authors

Eileen Doherty works as a Research Fellow in IVI. Her work involves researching a variety of subject areas – including Strategic Planning (SP), Technical Infrastructure Management (TIM) and Research, Development and Engineering (RDE) – and the development of academic publications that pertain to IT-CMF. Eileen has recently completed her PhD on *the adoption and diffusion of broadband technology by SMEs in Ireland*. She has nine years senior-level/ management experience in industry, specifically in the area of Business Information Systems (IS) and she has lectured in fields such as e-commerce, e-business, e-marketing, e-services, CRM and organizational behaviour. Eileen can be contacted at eileen.doherty@nuim.ie.

Dr Marian Carcary is a Research Fellow at IVI. She is lead researcher on three IT-CMF Critical Capabilities, including the Risk Management CC, and she also works on other IVI and EU-funded projects. Prior to taking up this position, Marian taught in the Kemmy Business School in the University of Limerick and worked as a part-time member of Faculty in the Limerick Institute of Technology for six years. She has completed MSc and PhD research, both of which were funded by scholarships from the Irish Research Council for Science, Engineering and Technology (IRCSET). Marian can be contacted at marian.carcary@nuim.ie.

Gerard Conway works as a Senior Research Fellow in IVI. His work involves researching a variety of subject areas – including Cloud Computing, Sustainable ICT (SICT), Business Process Management (BPM) – and the development of academic publications that pertain to IT-CMF. Prior to taking up this position, Gerard gained over 30 years experience in the IT industry. Before joining IVI, he was a researcher with DERI (Digital Enterprise Research Institute) at NUI Galway and prior to this he worked for Hewlett Packard as a manager with responsibility for delivering complex integrated global IT solutions. Gerard can be contacted at gerard.conway@nuim.ie.

This executive briefing was edited by Thomas Keogan of TeKcomm Technical Writing.

About IVI

The Innovation Value Institute (IVI) is a multi-disciplinary research and education establishment co-founded by the National University of Ireland Maynooth and Intel Corporation. IVI develops frameworks to assist IT and business executives to manage IT for Business Value and to deliver IT-enabled business innovation. IVI is supported by a global consortium of like-minded peers drawn from a community of public and private sector organizations, academia, analysts, professional associations, independent software vendors, and professional services organizations.

Contact Us

For more information on IT-CMF, cloud computing and risk management, or on becoming a member of the IVI Consortium, please visit www.ivi.ie or contact us at: ivi@nuim.ie or +353 (0)1 708 6931