25th Bled eConference
eDependability:
Reliable and Trustworthy eStructures, eProcesses, eOperations and eServices for the Future
June 17, 2012 – June 20, 2012; Bled, Slovenia

A Framework for the Evaluation of CloudSourcing Proposals

Roger Clarke

Xamax Consultancy Pty Ltd, Australia
Visiting Professor, Australian National University
Visiting Professor, UNSW, Australia

Roger.Clarke@xamax.com.au

Abstract
Many organisations have recently adopted variants of cloud computing. Many of them have done so with considerable enthusiasm, but with very little reflection. Commentators have warned of uncertain benefits, predictable disbenefits and a wide range of risks. A study of IT media reports shows that cloud outages are frequent, and that at least some of the theoretical risks are very real. This paper draws on the accumulated bodies of theory on outsourcing and information and IT security in order to propose an evaluation framework. This instrument supports an organisation's executives in evaluating proposals for cloud computing, and assists their governing Boards to fulfil their legal obligations to ensure that choices are informed by business case analysis and risk assessment.

Keywords: Cloud Computing, Outsourcing, Security, Business Case, Risk Assessment, Evaluation Framework

1 Introduction

Cloud computing emerged during 2006-09 as a fashion item. There is considerable scope for debate about what constitutes cloud computing, to what extent it is a technology, a service or a marketing buzz-phrase, and how it differs from its predecessors. Nonetheless, since 2009, various forms of cloud computing have entered the mainstream. Evidence of this includes the volume of business reported, the number of startups, and the number of established outsourcing providers that are launching cloud services.

Two of the three broad categories of offerings are intended specifically for sale to corporations and government agencies. Infrastructure as a Service (IaaS) refers to the provision of a bare (but virtualised) machine, with little more than a specific operating system and version. Amazon's EC2 and Rackspace were early movers in a marketspace that is becoming densely populated. Platform as a Service (PaaS), on the other hand, offers a configured platform on which organisations can install their applications.

Examples include Microsoft Windows Azure, Google Apps and a range of services offering specific application development environments.

The third category, Software as a Service (SaaS), makes specific application software available. SaaS is targeted at individual consumers as well as being offered to organisations as an alternative to applications running on the organisation's own hosts, or on their employees' workstations. Examples include Google Gmail, Google Docs, MS Live and Office 365, Dropbox and MYOB LiveAccounts.

Consumer needs of cloud computing have been considered in a parallel research project (Svantesson & Clarke 2010, Clarke 2011). The focus of the research reported on in this paper is on corporate rather than consumer use. The work builds on prior research that has been conducted into the requirements of user organisations for cloud architecture (Clarke 2010a), and the benefits and risks of cloud computing (Clarke 2010b).

Despite marketers' upbeat tone, there are many signs that all is not well, and that the many warnings that have been given by business and legal commentators are not being heeded. For example, the market-leading IaaS service, Amazon ECS, suffered a major outage in April 2011 (e.g. Dignan 2011). In addition to affecting user organisations that depended on the service, this undermined several PaaS providers. In the SaaS arena, there have been continual outages of Google's various services and of MS Live and MS Office 365, notably in September 2011. Salesforce's CRM and Intuit's accounting services have also caused considerable heartburn to SME clients on several occasions (e.g. Whiting 2010). In May 2011, it became apparent that the cloud is also now mainstream for criminal behaviour, with Amazon's cloud being used as a launch-pad for an attack on Sony's Playstation network (Galante 2011).

This leads to some important questions, including: Is cloud computing ready for 'prime time'? And is it appropriate for organisations to place reliance on IaaS, PaaS and SaaS providers? In order to address such questions, it is first necessary to answer some preliminary questions, importantly: On what basis can the judgement be made as to whether cloud computing is sufficiently reliable? And what complementary actions are needed by organisations that adopt it?

The purpose of this paper is to draw on relevant theories in order to propose an evaluation framework for cloud computing, and throw light on the framework by means of a review of provider reliability as disclosed by media reports of outages.

2 Research Method

A graphical representation of the approach adopted is in Figure 1. Two well-established bodies of theory provide a solid basis for evaluating the adequacy of cloud computing. One is that relating to the security of corporate IT. Security is used here to encompass the confidentiality, integrity and availability of both data and services. This is briefly summarised in the subsequent section.

The various *aaS offerings are variants of the longstanding concept of outsourcing. In conventional outsourcing, a supplier hosts equipment on which a relevant stack of software runs and data is stored and maintained. In cloud computing, the supplier changes the focus of the offer from the equipment to the processes. Those processes may be run in any of a wide range of devices, and the location of those devices is determined by the needs of the supplier, not those of the customer. The supplier scales

the number of processes and the processing speed and storage capacity to meet the customer's varying needs over hourly, daily, monthly and annual cycles, to reflect growth and decay factors, and in the face of demand uncertainty. The supplier may offer a tariff based on usage, because instead of unused capacity being locked up in hosts pre-allocated to a customer, the supplier can make more efficient use of the available computing resources.

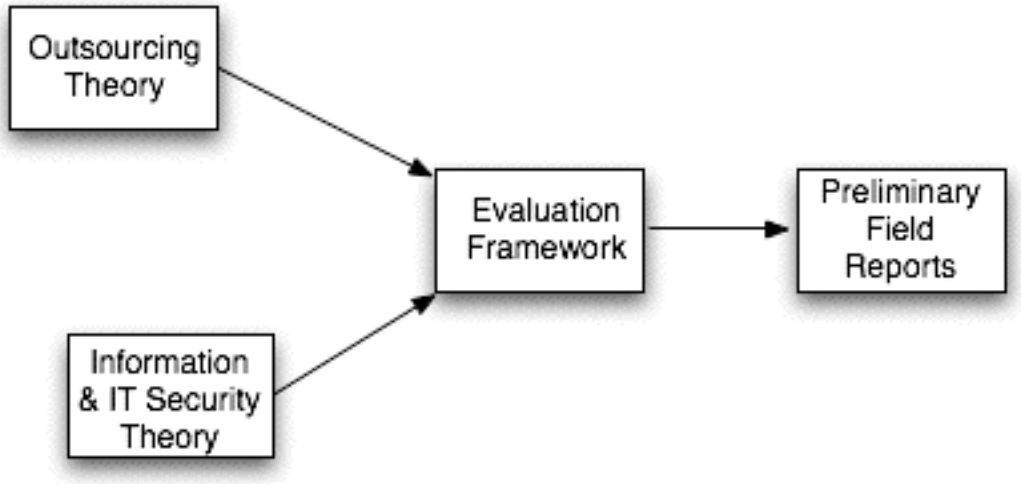

Figure 1: The Research Approach Adopted

A later section briefly summarises relevant aspects of the theory of outsourcing. To reflect the close association, the remainder of this paper uses the term 'cloudsourcing' to refer to all of the *aaS variants.

On the basis of these bodies of theory, combined with the technical media and the insights gained through the author's consultancy activities in the area, structured checklists are proposed, that can be used for assessing cloudsourcing proposals. One checklist lists the Benefits that may be able to be achieved, and the other focusses on Disbenefits and Risks.

The framework needs to be assessed to ensure it is relevant, understandable, practicable and comprehensive. It needs to be pilot-tested by being applied in a variety of organisational settings. Deep case studies need to be prepared. In order to gain insights into the framework's comprehensiveness, and its efficacy as a management tool, this paper reports on the outcomes of a preliminary test of the comprehensiveness of the 'Disbenefits and Risks' checklist. This was performed by scouring the technical media for reports of cloud outages, examining them, and viewing them through the lens provided by the framework.

The empirical component of the research of course has deficiencies. Media reports are selective, limited to a single perspective, in many cases strongly influenced by either a marketing organisation or a user organisation, almost always cross-sectional rather than longitudinal, and frequently shallow. On the other hand, technical media outlets have a strong motivation for exposing problems, because that is the way to gain attention, and attention is a critical factor in revenue-generation for contemporary media.

A further consideration that speaks in favour of media reports is timeliness. Formal case studies require considerable time to gather and analyse deep information on a rigorous basis. They involve compromise in order to gain access and approval for

publication (e.g. through anonymisation and even a degree of falsification), and they may be the subject of long delays in publication. The field is moving quickly, and researchers have an obligation to complement rigorous research with (cautious) utilisation of such information as is available in order to provide relevant information promptly.

The empirical component of this research offers value, but must be considered with care, and complemented by further studies, and its necessarily tentative conclusions must be reviewed as further information comes to hand.

3 Outsourcing and the Cloud

The term 'outsourcing' has long been applied to the acquisition of IT services from suppliers, as distinct from performing the tasks internally. Internally-delivered services have been retro-fitted with the term 'insourcing'.

Various sub-categories of outsourcing have been distinguished during the quarter-century of research on the topic, importantly:

- domestic (within-nation) outsourcing from cross-border (sometimes called 'off-shore') outsourcing – which increases the contractual challenges by adding cross-jurisdictional and perhaps also cross-cultural and multi-lingual issues
- hosting, 'utility computing' and Application Service Provision (ASP), each of which delivers services at a different level of the hardware, systems software and applications software stack
- IT outsourcing (e.g. equipment hosting) and business process outsourcing (e.g. the contracting-out of call centre operations)

Few refereed articles on outsourcing have to date addressed cloud computing. One important reasons is that it is a largely empirical literature and hence follows developments in the industry rather than leading them. However, Schwarz et al. (2009) considered that "Cloud computing has the same key attributes as the 'standard' ASP model" (pp. 750). See also Willcocks & Lacity (2012). The Schwarz et al. conception was that cloud computing "encompasses any subscription-based or pay-per-use service delivered over the Internet" (p. 751). Contemporary understanding of cloud notions is that there is an important additional criterion – server virtualisation. Their analysis does not appear to be invalidated by that factor, however, provided that it is appreciated that the risk factors inherent in cloudsourcing include not only those for ASP, but generally also those for cross-border outsourcing:

> *"Customer-perceived risks for both domestic and offshore outsourcing revolve around cost escalation (paying more than expected) and service debasement (delivered services are of lower quality than expected). However, offshoring introduces additional communication risks, exacerbated by distance and, often, language and culture differences, and additional cost risks associated with higher than expected communication, coordination, and control costs" (Schwarz et al. 2009, p. 752).*

A factor that is under-played in that quotation is the cross-jurisdictional issues such as compliance with the outsourcer's domestic laws about data protection, and enforceability of the supplier's undertakings in relation to service quality and data

security. With virtualised servers, user organisations have no way of knowing the jurisdictional location in which services are performed. That has the implication that, in most cases, user organisations also have no way of ensuring that processing is limited to jurisdictions that have been approved by parliaments whose laws they are subject.

A further source of insights arises in the smaller literatures on predecessor notions to IaaS, including grid computing (e.g. Neumann et al. 2007, Messerschmidt 2009) and utility computing (e.g. Haried & Zahedi 2004, Bodenbenner et al. 2007).

The primary drivers of outsourcing are generally perceived to be "cost reduction, access to technological expertise and enabling focus on its own core competence", rather than needing to sustain and manage technical capabilities in-house (Bergkvist & Fredriksson 2008, citing Lacity & Willcocks 2001). However, there has always been considerable scepticism among both consultants and academics about the achievability of the claimed benefits. The 'myths' literature is traceable back to Lacity & Hirschheim (1993). Moreover, "there is a growing body of evidence collected by both consultants and researchers that significant numbers of outsourcing arrangements are indeed unsatisfactory" (Rouse 2006, p. 1).

Studies of outsourcing success and failure generally consider strategic, technological, economic and performance perspectives. The performance perspective includes factors such as service reliability and quality. The dominant success factor examined in the empirical literature has been cost savings, with less attention given to service-quality, and very little consideration of longer-term factors such as fit, lock-in and adaptability. However, Rouse (2008) found that "only a minority (42%) reported cost savings ... There are several studies in the literature that corroborate the low likelihood of obtaining cost savings, and the reasonable possibility that costs will, in fact, rise ... Strategic, technology and economies-of-scale benefits had even lower success rates, as did overall evaluations of outsourcing satisfaction/value. In some respects these findings are even more disquieting than those related to cost savings" (p. 11).

Sullivan & Ngwenyama (2005) identified the main risk factors in several government agencies as being outsourcer's experience, opportunistic behaviour by the vendor, vendor experience, vendor financial responsibility, vendor performance monitoring, contract horizon and technological discontinuity, and loss of core competencies and proprietary information. A recent paper focussed on technical factors underpinning service quality, extracting 757 risk items from 68 papers, and reducing them to 70 technological risk items within 9 risk categories: IT Security, Confidentiality, Integrity, Availability, Performance, Accountability, Reliability, Maintainability, Regulatory (Ackermann et al. 2011). See also Lacity et al. (2010) and Lacity et al. (2011). The evaluation framework presented below reflects the insights from that literature.

It is clear from the outsourcing literature that cloud computing is a variant of outsourcing that includes server virtualisation, and hence that a great deal of accumulated insights and expertise from the outsourcing literature is capable of being applied, albeit with some care, to 'cloudsourcing'. It is also clear that outsourcing seldom lives up to the marketing hype, or even to outsourcers' hopes. Given the additional complexities and challenges inherent in cloud computing, it appears to be unwise for user organisations to anticipate that cloudsourcing will be a smooth ride.

4 Security and the Cloud

The term 'security', in the context of information, IT and services dependent on IT, is used in two distinct ways:

- security is a desirable condition in which harm does not arise, despite the occurrence of threatening events ('our customers enjoy a high degree of security'); and
- security is a set of safeguards designed to achieve that condition ('we have appropriate security in place')

The conventional security model involves Threats impinging on Vulnerabilities and resulting in Harm to Assets, but with Safeguards used to address the Risks.

The Assets that suffer harm may be defined as narrowly as information and IT artefacts. Alternatively, the scope of relevant Assets may be defined much more broadly, to encompass service-quality, human safety and privacy, the capacity of corporate stakeholders to comply with applicable laws and with its own stakeholders' expectations, and the wellbeing of the organisation, its stakeholders, or the economy and society as a whole. Depending on the scope of the Assets definition that is used, the focus may be on confidentiality, integrity and availability, or the concerns may extend to commercial matters, and to compliance issues.

For many organisations, the IT and associated processes that are being outsourced are fundamental to their operations, their success or failure, and even their very existence. The previous section noted how cloudsourcing exacerbates the risk profile, because is blends ASP with cross-border sourcing, and virtualises servers to the point that their location is neither readily knowable nor readily predictable. It is therefore essential that the broadest interpretations of scope be applied.

A very substantial body of professional and commercial knowledge exists in this area, including a great many Standards issued by industry associations and by national and international standards bodies. The Standards documents are characterised by large scale, by unclear language and by hidden assumptions. The result is that they tend to obscure rather than to inform, and to deflect discussion into myriad esoteric by-ways, rather than enabling executives to identify and focus on the relatively few factors that are critical in any given decision-making context.

Most contributions in the academic literature on security address very specific sub- topics within the area. A study conducted in 2009-10 and reported on in Clarke (2010a and 2010b), drew on a wide range of sources to develop a checklist comprising 5 top- level, 20 mid-level and 24 further deeper-level 'disbenefits and risks' that balance comprehensiveness and clarity, on the one hand, against quantity, on the other. The most directly useful reference in support of the endeavour was Avizienis et al. (2004), although their approach required adaptation to reflect the user organisation's perspective. The evaluation framework presented in the following section encompasses those elements.

5 An Evaluation Framework

A variety of approaches are available to assist in conducting evaluations of the applicability of outsourced services. For example, SWOT Analysis can be applied, to assist in identifying the relevant Opportunities and Threats embodied in the outsourced service and the Strengths and Weaknesses of the organisation in relation to its adoption. A process more directly relevant in this context has become known by the biased term 'construction of a business case'. A classification scheme for business case techniques is provided in Clarke (2005).

This paper focuses on circumstances in which the sponsoring organisation's perspective dominates and the interests of other stakeholders are a secondary consideration; and in which the data available for analysis is mainly qualitative rather than quantitative. In this quadrant of the classification scheme in Clarke (2005), the primary techniques available are internal cost-benefit analysis and risk assessment. A brief review of cost- benefit analysis as applied by individual organisations is in Clarke & Stevens (1997). Risk assessment is a well-documented business technique, and the subject of formal international Standards.

The evaluation framework that is proposed in this paper comprises two checklists that can be used by organisations in order to identify relevant areas in which information can be collected and evaluated.

The checklists are provided at the end of this paper. Table 1 identifies benefits. Table 2 combines financial and other costs (collectively referred to as disbenefits) and risks.

6 Review of Media Reports on Cloud Outages

Earlier versions of these checklists have been published in refereed papers and consultancy reports, and have been successfully applied in specific contexts in the private and public sectors. The experience gained has been reflected in the structure and expression of the updated checklist entries in this paper. However, use of an instrument of this nature in the field lacks the rigour required to draw reliable conclusions about its comprehensiveness, validity and usefulness. Formal studies are needed, which involve users and a researcher independent from the instrument's originator, and some form of reference-point against which comparison can be made.

A technique was devised to utilise one kind of external reference-point, in order to conduct a test of the framework's comprehensiveness. A review was undertaken of media reports published between 2005 and 3Q 2011 on cloud computing outages, and reported on in Clarke (2012) and supporting documents. Over 150 articles were found, of which 105 proved to be relevant. These identified 49 events. Of those, 26 related to 10 SaaS providers, 7 events related to 5 PaaS providers, and the remaining 16 events related to 5 IaaS providers.

These media reports give rise to some doubts about the claimed benefit of Scalability. Cascade effects are prevalent, and in those circumstances the available resources may be unable to scale enough, or quickly enough. The reports also underline the dependence of the quality of Scalability not only on processors but also on available bandwidth between processors, in order to support rapid replication of the databases on which the processes depend.

Because the reports relate to 'outages', they are mostly relevant to aspects of the Disbenefits and Risks Checklist in Table 2. The primary concerns that they give rise to involve various elements of Service Reliability. Outages are not uncommon, and they may last for some hours. The seriousness of instances of Non-Availability varies among services and among customers. In some circumstances, short-term failures may not matter (e.g. where they occur during outside the customer's working-hours, or the service is ancillary to business rather than operational in nature). On the other hand, many IaaS and PaaS services appear to be critical to business operations, and many small businesses appear to have quickly become dependent on SaaS services for such business functions as email, access to data about their own customers, accounting and
even payments processing. In such circumstances, the impact of even short outages can be very substantial.

Organisations that choose to be dependent on remote services could be expected to have fallback arrangements designed, trialled and at the ready. These might take the form of alternative cloud suppliers. On the other hand, it is not in the interests of cloud- providers to facilitate churn away from themselves, and hence standards and protocols supporting inter-operability have been slow to emerge. At this stage, fallback procedures are therefore in many cases manual, or use local and possibly *ad hoc* computing tools, and in any case offer degraded service-levels to staff and customers.

Where fallback arrangements are used, the organisation cannot switch straight back to the service when it becomes available. It first needs to update the state of the remote database to reflect transactions conducted in the interim, before it can resume use of the cloud service. As a result, the delay in restoring the service may be multiples of the outage-period of the underlying cloud service. The service's Resilience, as measured by the delay before 'normal service is resumed', may therefore be poor. Media reports have seldom mentioned the Recoverability aspect.

Many organisations appear not to have invested the effort needed to implement fallback procedures, and their business is therefore 'in limbo' during outages. This will have varying degrees of negative impact on service-levels to their customers. In the case of for-profits, it will have at least some degree of negative impact on revenue, market- share and profitability, and after some amount of elapsed time it can be expected to result in business failure. On the other hand, when the service becomes available again, the business processes in such companies can generally be resumed immediately.

As regards Service Survival, few instances of suppliers ceasing operation have been reported so far. One exception was the drop.io file-sharing service, closed at 6 weeks' notice following takeover by Facebook. There have been many other closures, however, including Pownce and FitFinder (micro-blogging), Yahoo! Geocities (web- hosting), Yahoo! Photos, Yahoo! Briefcase (file-hosting), and (among a whole flotilla of 'impermanent betas') Google Video, Google Health and Google Buzz. An 'industry shake-out' is inevitable, in each sector, and perhaps quite soon in IaaS in particular. It remains to be seen what effect this will have, how graceful the withdrawals of services will be, and what protections for customer interests will be applied.

Several instances were reported in which the important quality of Data Survival was not satisfied. Brand-name was no protection, with Apple, Microsoft and Google (in the SaaS space) and Amazon (IaaS) all among the suppliers whose services lost customer data. Although none of these cases involved wholesale loss of data (as has occurred in a

few cases with conventional ISP services), the losses may have been survival- threatening for some organisations. Moreover, in only 1 of the 49 identified cases was any significant compensation paid.

A further disturbing feature of the media reports was the frequency with which suppliers have been uninformative and unresponsive to their customers' concerns. It appears that many providers have adopted business models in which cost-minimisation is the dominant strategy, the terms of service are customer-unfriendly, service-level warranties are avoided, and no respect is given to the Russian proverb popularised by Ronald Reagan – 'trust, but verify'. It remains to be seen whether minimum standards of terms of service, service-quality and information-provision will emerge, or whether they will only be available with 'premium services'.

All of the media reports that were found could be readily mapped onto the evaluation framework. The information they provided threw light on a number of criteria, but there was no apparent need for any substantive adjustments to it.

7 Conclusions

Organisations in many sectors are highly-dependent on information technology, to the extent that many would be completely unable to perform their business functions without it, and those that are for-profit enterprises would be unlikely to survive lengthy unavailability of the automated processes that support their operations.

The last two decades have seen a shift from direct control over information technology to contractual arrangements for the management of the hardware hosting, and to a lesser extent to outsourcing of the business functions of managing the applications and even maintaining the application software.

A further phase in outsourcing has been under way for several years. The technical difference between longstanding forms and cloudsourcing is the 'virtualisation' of servers. A rational approach would see existing outsourced arrangements migrated to cloud solutions in an orderly manner, retaining the carefully devised and customised conditions that manage the particular risks that the organisation faces. Instead, there has been a tendency for organisations to adopt new services abruptly, accepting whatever terms the provider stipulates.

Many warnings have been given by commentators, in the business and IT press, and in the legal, commercial and information systems management literatures. The survey of media reports of cloud outages reviewed in this paper confirms that a considerable number of these risks are not merely theoretical, but real, and in some cases reasonably common.

Company directors have a legal responsibility to ensure that business risk is assessed and managed. In any IT-dependent organisation, that translates into a legal responsibility to ensure that information and IT risks are assessed and managed. Executives need to undertake careful evaluations of proposals to shift from insourcing
and conventional outsourcing to cloudsourcing. The framework proposed and evaluated in this paper provides a basis for executives to assist directors in fulfilling their responsibilities.

Table 1: Benefits Checklist

Enhanced version of a model first proposed in Clarke (2010a)

TECHNICAL BENEFITS

Scalability
Assured server-capacity, storage-capacity, and access to the requisite application software, even where transaction and/or data-volumes vary significantly over time

Professionalised Backup and Recovery
Assured backup of data and software, and assured, simple and efficient recovery, saving the organisation the need to itself act in a professional and disciplined manner, and remain attentive to the task

Copyright Convenience
Assumption of responsibility for all aspects of acquisition, maintenance and licensing of software and of data

Collaboration Convenience
Assured and convenient access to collaborative content (including data and documents that are co-owned and co-maintained by multiple authors)

ENHANCED SERVICE ACCESSIBILITY

Access to Services that are Otherwise Unavailable
Access to a new or exclusive capability
Access to an application that the user organisation is unable, for technical or financial reasons, to establish and run for itself

Access to Services from Devices in Multiple Locations
Access from multiple devices, in various locations, including at home, at work, at clients' sites, in airport lounges, and in Internet cafes

Access to Services from Scaled-Down Devices
Access to services on devices such as handhelds, mobile phones and tablets

Access to Services from Multiple Device-Types
Access from device-types with different characteristics and user-interfaces (such as desktop PCs, portable PCs, handhelds, mobile phones and tablets)

BUSINESS BENEFITS

Early Commencement of Application Development
The platform needed to support the development process may be readily available from a service-provider, removing the need for an acquisition, installation and configuration process

Rapid Launch of New Services.
The platform needed to support the operational process may be readily available from a service-provider, removing the need for an acquisition, installation and configuration process

Operational Costs that Reflect Usage
A project with a modest budget may be able to be deployed for low cost, with budget supplementation sought in the event that capacity needs to be increased due to rapid uptake by organisational users or by external users such as business enterprises, community organisations and/or citizens

FINANCIAL BENEFITS

Lower Investment / Up-Front Cost

Relief from the responsibility for, and investment in hosts, hosting software, applications, and people with the requisite expertise to establish the service and/or lower prices through economies of scale and/or scope.

Costs that cannot be avoided include effort, time and money to determine requirements, evaluate alternative ways of satisfying them, establish a strategy and plan, and implement, monitor and control performance against plan

Lower IT Staff Costs

Avoidance of the need to sustain and manage specialist skills in-house

Lower cost of access to expertise and skills, by renting them only when they are needed

Lower Operational Costs

Pay-per-use, in arrears, rather than payment in advance, including for excess capacity

Lower costs through economies of scale and/or scope that are greater than the supplier's profit-margin

Fit to Financial Management Philosophy. For some organisations, there may be advantages in the switch from Capital Budget / CAPEX to Recurrent Budget / OPEX, displacement of staff-count from the organisation's accounts to providers and/or replacement of complex 'Whole of Life' Costing with simpler 'pay-per-use' charges

Table 2: Disbenefits and Risks Checklist

Enhanced version of a model first proposed in Clarke (2010a)

OPERATIONAL DISBENEFITS AND RISKS

These items are expressed as desirable qualities that may be compromised

Fit – correspondence to the organisation's needs, including the functions performed, the business processes supported, the data model underlying them, communication protocols, data formats

Reliability – continuity of operation

- **Availability** – readiness and responsiveness of the services
- **Accessibility** – readiness and responsiveness of relevant networks, and delivery to all relevant device-types
- **Usability** – appropriateness of user interfaces, response-times, and consistency of response-times
- **Robustness** – frequency of planned and unplanned unavailabilities
- **Resilience** – speed of resumption after outages
- **Recoverability** – service readiness after resumption, including the incorporation of data captured during outages under fallback arrangements

Integrity – sustained correctness of the service, and of the data

Maintainability – fit, reliability, and integrity after bug-fixes & modifications

CONTINGENT RISKS

These items are expressed as undesirable outcomes

Major Service Interruptions

Supplier Collapse or Withdrawal of Service
Safeguards include software escrow; data backup/mirroring/synchronisation on the organisation's own site; escrow inspection; proven recovery procedures; rights that are proof against actions by receivers

Loss of Data
Safeguards include data backup/mirroring/synchronisation

Denial of Access to Data
Threats include blockage by competitors, opponents or a foreign power

Loss of Compatibility of software, versions, protocols, or data formats

Lack of Flexibility, for:

- Customisation
- Forward-Compatibility – to migrate to new levels
- Backward-Compatibility – to protect legacy systems
- Lateral Compatibility – to enable dual-sourcing and escape to an alternative provider

SECURITY RISKS
These items are expressed as desirable qualities that may be compromised

Service Security
The location of threats may be environmental, second-party and third-party, and they may affect any aspect of Reliability or Integrity

Data Security
The location of threats may be environmental, second-party and third-party, and they may be to content in remote or local storage or in transit

Authentication and Authorisation
The provision to appropriate users of convenient access to data and processes in the cloud, while denying access to unauthorised parties, including imposters who are actively seeking to circumvent safeguards

Resistance to Denial of Service Attacks
Safeguards include multiple, distributed servers, choke-point avoidance, and collaborative arrangements with upstream carriage service providers

COMMERCIAL DISBENEFITS AND RISKS
These items are expressed as undesirable outcomes

Acquisition

- Lack of Information
- Non-Negotiability of Terms and SLA
- High Entry-Costs

Ongoing

- Loss of Corporate Expertise re apps, IT services, and costs
- Inherent Lock-In Effect, from high switching costs, and unusual formats and protocols
- High-Volume Data Transfers, from large-dataset replication/synchronisation
- High Operational Costs

Low Quality of Service to the Organisation's Customers

COMPLIANCE DISBENEFITS AND RISKS
These items are expressed as legal requirements, subject to civil and/or criminal actions

General Statutory & Common Law Obligations

- Evidence Discovery Law
- Financial Regulations
- Company Directors' obligations – asset protection, due diligence, business continuity, risk management
- Security Treaty Obligations

Confidentiality – incl. against foreign governments

- Strategic
- Commercial
- Governmental

Privacy – particularly Unauthorised Use and Disclosure
Threats include Second-Party (service-provider abuse), Third-Party ('data breach', 'unauthorised disclosure'), Storage in Data Havens

References

Ackermann T., Miede A., Buxmann P. & Steinmetz R. (2011) 'Taxonomy of Technological IT Outsourcing Risks: Support for Risk Identification And Quantification' Proc. ECIS 2011, Paper 240, at http://aisel.aisnet.org/ecis2011/240

Bergkvist L. & Fredriksson O. (2008) 'Outsourcing Terms: A Literature Review from an ISD Perspective' Proc. ECIS 2008 , Paper 129, at http://aisel.aisnet.org/ecis2008/129

Bodenbenner P., Stößer J. & Neumann D. (2007) 'A Pay-as-Bid Mechanism for Pricing Utility Computing' Proc. Bled eConference, Paper 10, at http://aisel.aisnet.org/bled2007/10

Clarke R. (2005) 'Business Cases for Privacy-Enhancing Technologies' Proc. 5th Workshop on Privacy-Enhancing Technologies, Cavtat, Croatia, 2 June 2005. Revised versions republished as Chapter 7 in Subramanian R. (Ed.) 'Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions' IDEA Group, 2008, pp. 135-155, and as Chapter 3.15 in Lee I. (Ed.) 'Electronic Business: Concepts, Methodologies, Tools, and Applications' (4 Volumes), IDEA Group, 2008, PrePrint at http://www.rogerclarke.com/EC/PETsBusCase.html

Clarke R. (2010a) 'User Requirements for Cloud Computing Architecture' Proc. 2nd Int'l Symposium on Cloud Computing, Melbourne, May 2010, at http://www.rogerclarke.com/II/CCSA.html

Clarke R. (2010b) 'Computing Clouds on the Horizon? Benefits and Risks from the User's Perspective' Proc. 23rd Bled eConference, Slovenia, June 2010, at http://www.rogerclarke.com/II/CCBR.html

Clarke R. (2011) 'The Cloudy Future of Consumer Computing' Proc. 24th Bled eConference, June 2011, at http://www.rogerclarke.com/EC/CCC.html

Clarke R. (2012) 'How Reliable is Cloudsourcing? A Review of Articles in the Technical Media 2005-11' Forthcoming in Computer Law & Security Review 28, 1 (March 2012), PrePrint at http://www.rogerclarke.com/EC/CCEF-CO.html

Clarke R. & Stevens K. (1997) 'Evaluation or Justification? The Application of Cost/Benefit Analysis To Computer Matching Schemes' Proc. ECIS'97, Cork, Ireland, 19-21 June 1997, PrePrint at http://www.rogerclarke.com/SOS/ECIS97.html

Dignan L. (2011) 'Amazon outage ends cloud innocence' ZDNet, 23 April 2011, at http://www.zdnet.com.au/amazon-outage-ends-cloud-innocence-339313776.htm

Galante J. (2011) 'Sony Network Breach Shows Amazon Cloud's Appeal for Hackers' Bloomberg, 17 May 2011, at http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html

Haried P. & Zahedi F. (2004) 'The Next Phase of IT Outsourcing - Utility Computing: Understanding Utility Computing Acceptance' Proc. AMCIS 2004, Paper 436, at http://aisel.aisnet.org/amcis2004/436

Heiser J. (2011) 'Yes, Virginia, there are single points of failure' Gartner Blog, 30 May 2011, at http://blogs.gartner.com/jay-heiser/

Lacity M. C. & Hirschheim R. (1993) 'Information Systems Outsourcing: Myths, Metaphors and Realities' Wiley, Chichester, England

Lacity M. & Willcocks L. (2001) 'Global IT Outsourcing - In Search for Business Advantage' John Wiley & Sons Ltd, Chichester

Lacity M.C. , Khan S., Yan A. & Willcocks L.P. (2010) 'A review of the IT outsourcing empirical literature and future research directions' Journal of Information Technology 25, 4 (2010) 395-433

Lacity M.C., Solomon S., Yan A. & Willcocks L.P. (2011) 'Business process outsourcing studies: a critical review and research directions' Journal of Information Technology 26, 4 (December 2011) 221-258

Loh L. & Venkatraman N. (1995) 'An Empirical Study of Information Technology Outsourcing: Benefits, Risks, and Performance Implications' Proc. ICIS 1995, at http://aisel.aisnet.org/icis1995/25

Messerschmidt C.M. (2009) 'Adoption of Grid Computing: An Empirical Verification of an Inter- and Intra-Organizational Approach' Proc. PACIS , Paper 3, at http://aisel.aisnet.org/pacis2009/3

Neumann D., Stoesser J. & Weinhardt C. (2007) 'Bridging the Grid Adoption Gap – Developing a Roadmap for Trading Grids' Proc. Bled eConference Paper 22, at http://aisel.aisnet.org/bled2007/22

Reese G. (2011) 'The AWS Outage: The Cloud's Shining Moment' O'Reilly, 21 April 2011, at http://broadcast.oreilly.com/2011/04/the-aws-outage-the-clouds-shining-moment.html

Rouse A. (2006) 'Explaining I.T. Outsourcing Purchasers' Dissatisfaction' Proc. PACIS 2006, Paper 1, at http://aisel.aisnet.org/pacis2006/1

Rouse A. (2008) 'Testing Some Myths About IT Outsourcing: A Survey of Australia's Top 1000 Firms' Proc. ECIS 2008 , Paper 80, at http://aisel.aisnet.org/ecis2008/80

Schwarz A., Jayatilaka B., Hirschheim R. & Goles T. (2009) 'A Conjoint Approach to Understanding IT Application Services Outsourcing' J. Assoc. Infor. Syst. Volume 10, Issue 10, Article 3, 748-781, October 2009

Sullivan W.E. and Ngwenyama O. (2005) 'How Are Public Sector Organizations Managing IS Outsourcing Risks? An Analysis of Outsourcing Guidelines from Three Jurisdictions' Journal of Computer Information Systems XLV, 73-87

Svantesson D. & Clarke R. (2010) 'Privacy and Consumer Risks in Cloud Computing' Computer Law & Security Review 26, 4 (July 2010) 391-397

Urquhart J. (2010) 'The 'Cloud Computing Bill of Rights': 2010 edition' Cnet News, 7 June 2010, at http://news.cnet.com/8301-19413_3-20006756-240.html

Wainewright P. (2009) 'Sage shows why bigcos can't be trusted with SaaS' ZDNet, 11 February 2009, at http://www.zdnet.com/blog/saas/sage-shows-why-bigcos-cant-be-trusted-with-saas/655

Whiting R. (2010) 'Intuit Services Outage Draws Angry Comments From SMBs' CRN, 17 June 2010, at http://www.crn.com/news/applications-os/225700462/intuit-services-outage-draws-angry-comments-from-smbs.htm

Willcocks L. & Lacity M. (2012) 'Outsourcing Practices Reconsidered: From IT to Cloud Services' Palgrave Macmillan, 2012