Abstract—While much-hyped, cloud computing offers early adopters potentially significant benefits. However, important barriers to adoption have also been identified. This paper canvasses and discusses the ‘state of play’ of cloud computing risks. The paper reviews and compares ‘state of practice’ views on cloud computing adoption risks with ‘state of art’ research, based on commentary evidenced in a sample of blogs, industry press articles, white papers and industry presentations and a sample of research journal articles, respectively, published from January 2009 to September 2010. Gaps between the two are identified and discussed and conclusions drawn about cloud computing adoption, adoption risks, and research directions.

Keywords—cloud computing, adoption, risks, barriers, benefits

I. INTRODUCTION

A year ago, clouding computing was still a curiosity piece, attracting zealotry and derision aplenty. Today, it is seen by many as the next wave of IT, expected to change the economics and strategic direction of corporate IT [17]. Indeed, Gartner predicts that by 2012, 20% of businesses will own virtually no IT infrastructure [12]. The global world cloud computing market is currently estimated to be worth more than US$20 billion [1] and is expected to grow to over US$44 billion by 2013 [6].

Claimed benefits of cloud computing include: on-demand service; convenient pay-as-you-go billing; scalability (up and down); facilitates rapid start-up; minimizes start-up costs (minimal infrastructure setup) and reduces operating costs (use only what you need); anytime, anywhere availability; facilitates user mobility and collaboration (through shared data and applications stored in the cloud); reduces IT capital expenditure requirement; frees-up IT resources for other priorities, and; enables innovative new business services and models. Furthermore, many advocates believe that these benefits are only the tip of the iceberg of what cloud computing will deliver over the next ten years [17].

Others, however, point to significant barriers to widespread adoption of cloud services. Cloud computing is immature and not yet ready for widespread adoption, especially for mission-critical enterprise use. For example, a survey in March 2010 of ISACA’s (Information Systems Audit and Control Association) Oceania members found that 49% of respondents believe that the risks of cloud computing outweigh the benefits, and 30% have no plans to use clouding computing for any IT services [8].

Furthermore, KPMG’s 2010 global survey of CIOs found that while 72% of respondents see cloud computing as an IT sourcing option, their preference was for deployment of non-critical systems. KPMG’s view is that cloud computing use for critical systems and data is five to ten years out [9]. Gartner, however, is more bullish. It sees cloud computing being enterprise-ready by 2015. Gartner predicts that growth will be in three phases: by 2011 early adopters will engage the cloud for tactical projects; 2010 to 2013 will be about market consolidation, and; 2012 to 2015 will see mainstream critical mass and commoditization, and widespread adoption beginning to occur [16]. Gartner believes that open source cloud technologies will emerge by 2014. At that time, cloud computing will be the preferred but not exclusive choice for the majority of “opportunistic and architecturally simple application development efforts” by Global 2000 enterprises.

Cloud computing adoption risk has received little focus in the academic literature. This paper considers barriers to adoption (risks) by reviewing opinions by industry commentators (representing the ‘state of practice’) and comparing them to recent cloud computing research (representing the ‘state of art’). Gaps are identified and discussed, and conclusions are drawn about the ‘state of play’ of cloud computing adoption. The paper aims to cross-inform practice and research of each others’ issues of focus and provide direction in resolving adoption barriers.

II. STATE OF PRACTICE

This section examines practice-based adoption barriers.

A. Research Method

Cloud computing experience is underdeveloped as yet in the academic literature. Furthermore, as it does emerge, it may not fully reflect the heightened expectations (‘hype’) of cloud computing found in the broader media. Therefore, for the state of practice, the study drew on a range of ‘social commentary’ about cloud computing adoption from blogs, industry press articles and presentations, and white papers. A convenience sample was chosen from emails received by the author from various listserv and other online subscriptions relating to material published between January 2009 and September 2010, inclusive. A total of 320 items were examined from which 109 were selected as relevant to the topic. Selected items discussed one or more risks, issues or barriers associated with cloud computing adoption (collectively referred to here as ‘risks’).
The selected items were examined for instances of these risks, which were compiled in a spreadsheet. A total of 437 risk factor instances were found in the sample items. The factors were then clustered into factor categories. Ten main risk categories emerged from this analysis as a manageable set for comparison and presentation. The categories cluster related risk factors as follows:

1. **Security** – security, privacy, confidentiality, access control, visibility, transparency (data and applications).
2. **Lock-in** – vendor and technology lock-in, licensing, migration, interoperability, standards, architecture.
3. **Control** – control, monitoring, management, trust.
4. **Legal** – compliance, regulations, legal, contracts, audit.
5. **Service** – service provision, service level agreements (SLAs), support, availability, reliability.
6. **Performance** – latency, response time, execution time.
7. **Cost** – cost, economics, charging, charge-back, tax.
8. **Governance** – ownership, responsibility, business risk, due diligence, policy.
9. **Competencies** – competencies, knowledge, experience, skills, learning.
10. **Industry** – industry structure and rationalization.

Table I shows the frequencies and frequency percentages of the 10 risk factor categories, ranked from most to least frequent for the practice-based sample.¹

### B. State of Practice Findings

Table I indicates that the top five risks account for almost 84% of cloud computing adoption concerns. The top two risks (Security and Lock-in), account for nearly 47% of the total (nearly 24% and 23% respectively), while the next three risks (Control, Legal and Service), account for a further 37% (approx. 13%, 13% and 11% respectively). The remaining adoption concerns comprise Performance, Cost, Governance, Competencies and Industry factors.

<table>
<thead>
<tr>
<th>No.</th>
<th>Risk category</th>
<th>Practice</th>
<th>Research</th>
</tr>
</thead>
<tbody>
<tr>
<td>%</td>
<td>% Freq.</td>
<td>%</td>
<td>% Freq.</td>
</tr>
<tr>
<td>1</td>
<td>Security</td>
<td>23.8%</td>
<td>38.4%</td>
</tr>
<tr>
<td>2</td>
<td>Lock-in</td>
<td>22.9%</td>
<td>22.2%</td>
</tr>
<tr>
<td>3</td>
<td>Control</td>
<td>13.3%</td>
<td>8.1%</td>
</tr>
<tr>
<td>4</td>
<td>Legal</td>
<td>12.8%</td>
<td>11.1%</td>
</tr>
<tr>
<td>5</td>
<td>Service</td>
<td>11.0%</td>
<td>9.1%</td>
</tr>
<tr>
<td>6</td>
<td>Performance</td>
<td>5.0%</td>
<td>5.1%</td>
</tr>
<tr>
<td>7</td>
<td>Cost</td>
<td>5.0%</td>
<td>4.0%</td>
</tr>
<tr>
<td>8</td>
<td>Governance</td>
<td>3.7%</td>
<td>2.0%</td>
</tr>
<tr>
<td>9</td>
<td>Competencies</td>
<td>1.4%</td>
<td>0.0%</td>
</tr>
<tr>
<td>10</td>
<td>Industry</td>
<td>1.1%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>% Freq.</th>
<th>% Freq.</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.0%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

¹ The full list of risk factors (spreadsheet) and sample sources (references) for the state of practice dataset are available from the author upon request.

The practice data comprises a mix of expert opinions, industry surveys, hearsay and experience-based observation and commentary that is provided for a range of motivations including informing, advising and influencing. As such, it represents a broad spectrum of views about risks, issues and barriers to adopting cloud computing reflecting general current social and industry opinion.

Key risks within each category are outlined following.

1. **Security**. Security is typically ranked the top cloud computing adoption concern. Key threats include: abusive and nefarious usage; insecure interfaces and APIs; malicious insiders; shared technology issues; data loss or leakage; account or service hijacking, and; general uncertainty due to ‘security by obscurity’ [5].

Potential security attacks include denial of service attacks, side channel attacks, authentication attacks, man-in-the-middle cryptographic attacks, spyware and trojans [7]. For example, researchers applied a denial of service attack on a client company from hired EC2 instances, which was not detected by Amazon [11]. Also, researchers found that EC2 was susceptible to side-channel-attacks [13]. Quick easy access for customers also means quick easy access for attackers. More innocently, cloud instances have been found to contain authentication keys in the caches and credit card data, as well as the potential for malicious code to be hidden within the system [10].

Due to high levels of abstraction, it is difficult for users to know what their systems are doing in a public cloud and how they are being protected. The customer’s need for visibility and transparency of operation are at odds with the service provider’s need to efficiently manage entire data centers and maintain secrecy over its security measures.

Opinions vary on how serious this issue is. Some argue that security threats in the cloud are no greater than in on-premise data centers. Others argue that the level and quality of protection is better in the cloud due to the greater scale of operation and technical expertise of cloud computing providers. Some argue that security is a joint responsibility of the provider and customer while others claim that, ultimately, security can only ever be the customer’s responsibility. Some say the good news is that the same tools for internal security can be used for cloud security. Others say, however, that existing policies, procedures and tools must be extended and supplemented to cater for the particularities of cloud requirements. Many argue that the cloud is not yet a secure enough option for storing and processing mission-critical or customer-sensitive data, and may never be. Some argue that, regardless, competitive pressures will overcome many cloud risks because the economics of cloud computing are so strong – for providers and consumers – that widespread adoption is inevitable.

The Cloud Security Alliance [4] suggests that the issue varies with the cloud service model utilized. The lower down the service stack you go (SaaS, PaaS, IaaS), the greater the responsibility for security that the customer must assume:

- **SaaS** usually provides the most integrated offering, including a high level of security, with the least customer extensibility.
• *PaaS* is usually more extensible than *SaaS*, but offers fewer customer-ready features, including security features and capabilities, enabling/requiring the customer to layer-in needed security.

• *IaaS* provides enormous extensibility but few if any application-level features. Here, the customer must manage and secure the execution environment.

Finally, an additional challenge is to integrate cloud-based security with on-premise security. This raises issues of interoperability and standards, discussed next.

2. **Lock-in.** This category combines several critical risks with characteristics that could be positioned along a spectrum spanning fully proprietary through to standardized services. They include vendor lock-in, technology lock-in, migration, interoperability, architecture, licensing and standards. Due to the rapid emergence of cloud computing through the initiatives of individual companies, most offerings are highly proprietary in nature. This creates challenges in migrating data and applications to the cloud, or switching cloud providers, and puts customers at significant risk if the need arises for systems to interoperate across cloud and in-house environments or to retrieve data and/or applications if a cloud provider withdraws from the market. Furthermore, *SaaS* data may not be fully retrievable and applications developed on one *PaaS* may not be portable to, or executable on, another. There are few, if any, ready-mechanisms to migrate data and applications to other environments. Compatibility issues tend to increase up the service stack, as described above, reflecting the degree of provider-supplied integration (and, therefore, proprietary solutions and interfaces). Switching costs are high. Hence, vendor/technology lock-in.

A related aspect of cloud migration and interoperability is the architecture of existing applications (and data formats) intended to run in the cloud. There is a significant difference between an application running in a cloud environment and an application being able to benefit from cloud computing characteristics such as scalability and dynamism. To utilize the beneficial characteristics of the cloud, an application needs to be purpose-designed for the cloud (a kind of reverse lock-in or lock-out due to design/architecture). Similarly, to interoperate across hybrid environments, some customization is likely to be necessary. Typically, on-premise and legacy systems are not designed for horizontal scalability or mixed-mode execution. Auto-scaling infrastructure does not automatically make an application scale or elastic. To avoid these issues, companies need to learn how to build and run applications suited for cloud computing environments.

Portability requires standard interfaces but few standards exist as yet. The industry is still too immature. The question of standards, however, is contentious. Some argue that widespread adoption of cloud computing (especially by enterprise users) will remain limited until the problems of interoperability and lock-in are resolved. Others argue that a rush to standards could stifle innovation and constrain the industry from reaching the full potential of utility computing. Nonetheless, various cloud standards initiatives are already underway (see the cloud-standards.org wiki for details).

Finally, software licensing may be an issue, depending on the service and software utilized. Some licensing agreements are tied to a physical server and continuous use, making it difficult to move the software to the cloud or virtual servers. In general, this is a commercial matter that must be resolved on a case-by-case basis with each software vendor.

3. **Control.** This category comprises risks resulting from the reality that control over an organization’s data and systems execution ultimately passes to a third party service provider in cloud computing. This can raise important concerns and barriers to cloud adoption because a change in control means a change in risk. These concerns represent part of the downside to the benefits of cloud computing, resulting from not owning the infrastructure. What can be done is constrained by the permissions (rights) granted by the service provider.

A related concern is that effective cloud computing is likely to require increased automation, which creates an increased demand on management capabilities and increased risk as hands-on control is removed. Cloud computing adoption presents significant management challenges, not the least because of the limited availability of cloud monitoring and management tools and the limited capabilities of tools that do exist. For example, tools usually do not integrate with on-premise management tools. Also, existing tools handle applications poorly (compared to hardware and operating systems), especially multi-tiered applications.

Other control issues cited in the literature include the problem of instance sprawl. Users may spawn instances unnecessarily and wastefully, just because it is possible and easy. Related is the problem of keeping track of an organization’s overall usage of cloud services. If it is so easy and inexpensive for anyone in any department to ‘hop onto’ the cloud, aggregate costs may balloon.

Finally, some commentators also remind us of the human element in cloud computing. People can also feel a loss of control and resist change. Contrary to popular claims, there is a steep learning curve in cloud adoption. Also, it has been widely postulated that the IT function as we know it is under threat. As the need to maintain servers and other data center infrastructure diminishes, the form of the IT function may change. Staff cuts are likely. This can create a classic dependency where the success of transitioning to a new operating model is dependent upon the people who may become redundant as a result of the change.

4. **Legal.** Legal risks include compliance with jurisdictional laws and regulations, legal liability, contracts and audits. Depending on the nature of the data (and it could be as simple as emails) and the jurisdiction, regulations may apply to where data is stored, how it is handled, and the procedures under which it may be accessed or seized by the courts or governments. Special regulations often apply, for example, to personal details, financial data, and health records, or a requirement may exist for data to remain within a specific country. Cloud virtualization can cause data to be moved around cloud environments, placing it under different state and national laws and even result, unknowingly, in the owner becoming liable for breaches. *IaaS* providers, such as Amazon Web Service (AWS), typically let the
customer specify the domain in which data is to be stored, thereby mitigating some of this risk but this option is not necessarily uniformly provided across the service stack or by all service providers.

A key sticking point here is: Who is responsible for compliance? The service provider who processes and stores the data or the customer? Providers argue that they cannot be held responsible because they know nothing about the nature of the data or its compliance requirements. Customers, in turn, have no visibility into the provider’s infrastructure or handling of the data. However, a compliance/legal exposure can be created by a vendor leaking, breaching, losing, damaging or impeding access to data. Yet, the typical default contract from most cloud providers (such as AWS) puts the onus for compliance and privacy fully on the customer.

Furthermore, cloud vendors typically offer poor service guarantees and limited financial redress if their service fails (such as a percentage of the fees due). This may represent minimal value in comparison to the real cost of service loss to a customer. It is not always clear who is responsible when problems arise or how they will be resolved. Providers also usually claim the right to change their terms and conditions in contracts without notice, by posting them on their website. These issues are major barriers to adoption for enterprises and for moving mission-critical or data-sensitive applications to the cloud.

Finally, the cloud presents challenges for auditing, especially of customer data and systems. Traditional forms of auditing may not be possible or permitted by the provider. Alternative approaches may be necessary. Providers may deny access to auditors to protect other multi-tenanted users, to maintain secrecy over its security arrangements, or simply because it does not have the resources to allow each customer to inspect its systems or run audit programs outside of controlled hired instances.

5. Service. This category relates to service features and levels, service availability and reliability, and support. Clearly, quality and continuity of service are important considerations in adopting and continuing to use cloud services. Unfortunately, due to the utility nature of cloud computing, services and service levels are commodity-like in nature, with iron-clad guarantees on services, availability, reliability and support rarely provided. Typically, cloud service level agreements (SLAs) are inadequate, inflexible or nonexistent. Also, service scope varies between providers, partly as a result of differences in service model offerings and partly due to differing business policies. Limited options exist, if any, for customization of services.

For example, a customer has no visibility into his/her relative standing in the multi-tenant environment for support following an outage (who is brought online first?) or for receiving software updates as they become available. This is usually driven by the provider’s own priorities. Typically, only basic support is available from the cloud provider (such as AWS) with value-added services provided by third parties. Amazon does not provide end-to-end application support. It supports the compute infrastructure and leaves application support to the customer.

While the remaining five categories account for only 16% of the risk factors found, they still amount to substantial adoption barriers in the minds of some industry analysts.

6. Performance. Network latency, data access and storage latency, and overall response and execution times are important issues for some users and applications, given the view that system performance is slower in the cloud and more variable than in on-premise environments. Performance is constrained by Internet speeds, network quality and the distance between the user and the various cloud service providers. Tests show that latency increases with distance [14]. More alarmingly, studies have found that cloud platform performance varies substantially, by up to a factor of 20, depending on the time of day the service is accessed [18]. Performance is also influenced by other factors such as application design (they must be virtualized to operate efficiently in a cloud environment). Architecting applications for performance and scalability in the cloud is a non-trivial exercise [3]. So, if performance is critical in your service level requirements, the cloud may be a risky option.

7. Cost. One of the great benefits touted for the cloud model is that you only have to pay for what you use when you use it. Is it that simple in practice? Accurately predicting and measuring spend is more difficult under an ‘on-demand’ costing model. Knowing who used what services when in a large organization is also difficult to track. Add to that the uncertainty about whether the required instances were over-subscribed or under-utilized makes costing enormously difficult. The risk exists for firms to lose control and spend more than they need to under this model. Implications for charge-back to cost centers extend from these difficulties. Also, current prices are low, as vendors compete for market share. However, as the market grows and customers become locked-in, prices may rise. Finally, pay-per-use has financial and tax implications, as IT costs change from capex to opex, which can have positive and negative effects.

8. Governance. Governance involves issues of ownership, decision rights, responsibility, accountability, business risk, due diligence and business policy (such as relating to the control of sensitive data and the use of standards). Cloud computing upsets traditional IT governance arrangements because much of the control transitions to third parties. It can also change the internal structure of IT in user organizations, decentralizing much of the decision-making. This places pressure on the strategic function of IT at the center (head) of organizations. However, these issues do not necessarily weaken internal governance. Rather, they change its shape (its roles and responsibilities). Commentators argue that robust governance is an important entry requirement to benefit from the use of cloud services.

9. Competencies. While cloud computing draws on legacy client-server and service-oriented architectures, it represents a new bundling of preexisting technologies. Most potential adopters do not have the specific skills to build and deploy cloud applications as quickly and efficiently as the hype suggests is possible. There is a steep learning curve with this computing model. Furthermore, cloud service models and
platforms differ in their technical makeup and usage requirements so experiential-based learning can be a barrier to realizing benefits through cloud adoption.

10. Industry. Finally, several commentators note that cloud computing, as an industry, is immature so is likely to change over time as industry rationalization occurs. Costing, service models and cloud architectures/infrastructures may change. Providers (small or large) may fail, withdraw or be acquired, representing service continuity risks for customers. Risk-averse consumers may adopt a 'wait and see' strategy before joining the cloud market.

Based on these risks, in aggregate, current opinion is that cloud use cases are limited to: when demand is unknown, uncertain or highly variable; when data and applications are not tightly coupled with other data/apps or the points of integration are well-defined; when tight security and control are not so important; when availability and performance are not critical, and; when specific data regulations do not apply.

III. STATE OF ART

This section examines current research relating to cloud computing risks.

A. Research Method

Research papers on cloud computing adoption risks were selected by searching four online databases (ABI/INFORM Global, ScienceDirect, ACM Digital Library and IEEE Xplore) for items containing the words “cloud computing” and “risk” in the abstract from 2009 until September 2010. A total of 58 articles were retrieved, from which 32 were found to be relevant to the topic.

The articles were examined for instances of research relating to cloud computing adoption risks. A total of 99 risk factor instances were found and classified according to the same categories used for practice-based items. The ‘research’ column in Table I lists the frequencies and frequency percentages of the factors in each of the ten categories.²

B. State of Research

The first obvious difference to note between research and practice is the comparatively low number of research articles. In part, this may reflect the differences in sampling procedures. However, a separate search of the same databases for articles containing only “cloud computing” in the abstract found 1057 items, suggesting that only 3% (32/1057) explicitly address risks. The search criteria, however, may underestimate the level of research interest because other papers may address relevant adoption issues but not call them "risks". Nonetheless, there are prima facie indications that explicit risk-related studies may be underrepresented in cloud computing research.

Second, risk-related research is strongly biased towards security, disproportionately so in comparison to the relative interests of practice (38.4% versus 23.8%). This is, perhaps, not surprising given that practice considers security to be the top adoption risk. It may also be that security lies as the intersection of cloud computing’s characteristic technical features of virtualization, multi-tenancy, shared resource pooling, elasticity, web deployment, and utility service delivery, making it a complex issue to resolve, with many fronts. This view is supported by examination of the security issues being researched. No obvious pattern is discernible in the security issues currently studied. They span a broad range of topics including trusted data storage, identity management, security protocols, security attacks, virtual machine image management, and security assessment and compliance. A more formal overview of security issues from a service model perspective and review of current security solutions is provided in [15].

Third, the two lowest frequency practice risks (Competencies and Industry) receive no attention at all in the research literature examined. This suggests that, at present, consideration of people/skills issues and industry/market factors are low on research agendas.

Fourth, the other risks attract research attention in a consistent frequency order to that of practice, but lagging at a lower frequency rate by 1-2%, with the exception of Control, which lags practice by over 5% (and drops below Service in frequency order). This may reflect the possibility that current research is focused on solving technical, provider-side problems rather than customer-side management issues. Finally, focus on Performance is essentially the same (5%) in both domains.

Overall, the state of art reflects the reality that cloud computing is still at an early stage of development. Much research remains to be done on issues and risks that have already been identified. Also, new challenges continue to emerge as adoption ramps up and new use cases evolve. In the short term, however, the relative immaturity of current service models will likely dictate that research focuses on fundamental technical issues of service provisioning ahead of higher level customer concerns. For example, mapped against our risk categories, research challenges proposed in [19] are dominated by concerns with data center performance and cost efficiencies:

- **Data security** – the ability to secure data access, transfer, and storage and provide visibility of security integrity and tampering (Security).
- **Automated service provisioning** – the ability to acquire and release (allocate and de-allocate) resources on demand without manual intervention (Performance).
- **Virtual machine migration** – the ability to detect and avoid hotspots and balance data center load by migrating virtual machines quickly and efficiently (Performance).
- **Server consolidation** – the ability to save energy costs by migrating virtual machines from underutilized servers without compromising application performance or creating resource congestion elsewhere (Performance).
- **Software frameworks** – the need to improve performance and resource management in MapReduce frameworks (such as Hadoop) in heterogeneous environments (Performance).

² The full list of risk factors (spreadsheet) and sources (references) for this state of art dataset are available from the author upon request.
• **Storage technologies and data management** – the need to improve data handling in data-intensive tasks such as occurs under MapReduce (Performance).

• **Traffic analysis and management** – the ability to analyze, measure and manage data center traffic flows/patterns (Performance).

• **Energy management** – the need to improve energy efficiency in data centers (Performance).

• **Novel architectures** – research alternatives to the current dominant model of large scale data centers (Industry).

### IV. CONCLUSIONS

Several conclusions can be drawn about the state of play:

First, the barriers to adoption of cloud computing, in the form of currently perceived issues and risks, are high. Yet, the potential benefits are real, enticing and substantial. This is likely to prompt the gradual removal of many barriers. It is likely therefore that service maturation and industry stabilization will see the evolution of a range of beneficial services to meet the needs of a wide spectrum of IT users.

Second, current practice-based risks represent a range of real threats through to potential issues depending upon the service model adopted and the level of ‘savvy’ of the adopter. During these early years of the cloud product life cycle, successful adopters of cloud computing services will be informed and have realistic expectations. They will have invested the time and effort necessary to understand the capabilities of cloud computing (in contrast to the hype), and the risks, and have identified a suitable engagement strategy (Which services? Which apps? What controls? etc.).

Third, furthermore, successful adopters will recognize that there are many service model-specific learning curves to overcome in cloud service utilization. As a result, they will invest in developing experience and capabilities in using cloud services – initially, perhaps, through pilot projects. The practice of some early adopters of traditional IT outsourcing of effectively passing responsibility for all or parts of an organization’s IT function to the service provider is even less likely to work with the cloud than it did with conventional IT outsourcing. In the cloud, experience-based knowledge is power and the key to avoiding and mitigating the risks of adopting and using cloud services.

Fourth, according to the timeline suggested by Gartner (ca 2015) [16], the cloud environments that will attract widespread adoption probably do not exist yet. Service offerings and enabling technologies will continue to change and emerge. Realization of widespread adoption will depend on the innovation and research that is underway now. Therefore, learning curves will be both continuous (for evolutionary developments) and discontinuous (for new innovations) over the next five years, at least [2]. These changes will present ongoing challenges for adopters and may also introduce new adoption issues and risks not yet considered.

Fifth, based on the criticality of some identified risks for some potential customers, opinions that the cloud will result in radical de-scaling of the role of the enterprise IT function may be overstated, at least as a mainstream trend. The cloud/utility computing model may not meet all business or organizational computing requirements. Based on current indications, the longer term role of cloud computing is more likely to emerge as another sourcing option for IT services rather than as a replacement for all on-premise computing.

Finally, the study has limitations: the state of practice data was drawn from industry commentary rather than academic experience reports and sampling was not random; the field is developing so rapidly that it is very difficult for one researcher to span all available/emerging information, and; the scope was limited to adoption, at the expense of provision. However, these limitations provide opportunities for future research.

Cloud computing has tremendous potential to benefit organizations but substantial challenges and risks stand in the way of adoption. Research and practice must work together to mitigate the risks and realize the potential benefits of the cloud.

### ACKNOWLEDGMENT

NICTA is funded by the Australian Government as represented by the Department of Broadband, Communications and Digital Economy and the Australian Research Council through the ICT Centre of Excellence program.

### REFERENCES


