Using COBIT 5 for Risk to Develop Cloud Computing SLA Evaluation Templates

Conference Paper · September 2015

DOI: 10.1007/978-3-319-22885-3_21

3 authors:

Onyeka Illoh
Concordia University College of Alberta
1 PUBLICATION **6** CITATIONS
SEE PROFILE

Shaun Aghili
Concordia University of Edmonton
23 PUBLICATIONS **99** CITATIONS
SEE PROFILE

Sergey Butakov
Concordia University of Edmonton
70 PUBLICATIONS **364** CITATIONS
SEE PROFILE

Using COBIT 5 for Risk to Develop Cloud Computing SLA Evaluation Templates

Onyeka Illoh[1, 2,1], Shaun Aghili[1], and Sergey Butakov[1]

[1]Concordia University of Edmonton, Alberta, Canada

{shaun.aghili, sergey.butakov}@concordia.ab.ca

[2]Information Systems Assurance Management, Concordia University of Edmonton, Canada

o.illoh@yahoo.com

Abstract. The use of cloud services as a business solution keeps growing, but there are significant associated risks that must be addressed. Despite the advantages and disadvantages of cloud computing, service integration and alignment with existing enterprise architecture remains an ongoing priority. Typically, quality of services provided is outlined in a service level agreement (SLA). A deficient template for evaluating, negotiating and selecting cloud SLAs could result in legal, regulatory, and monetary penalties, in addition to loss of public confidence and reputation. This research emphasizes (or advocates) the implementation of the proposed SLA evaluation template aimed at cloud services, based on the COBIT 5 for Risk framework. A gap analysis of existing SLAs was done to identify loopholes, followed by a resultant template where identified gaps were addressed.

Keywords: Cloud computing, Cloud users, Cloud providers, Service level agreements, Software as a Service, Platform as a Service, Infrastructure as a Service, Everything as a Service, COBIT 5 for Risk.

1. Introduction

1.1 Background

Cloud computing remains a hot topic among vendors, enterprises and end users. Different authors and industry experts advocate a variety of approaches to realize benefits at optimal costs, and reduce associated risks from cloud computing [1, 2]. Some of the key benefits include: pay-as-you-go model, scalable solution that supports rapid business growth, cost transparency to the end user or business, outsourcing of compe-

[1] Corresponding Author

tencies that are not core to the business, as well as mirrored solutions to minimize the risk of downtime [1, 2].

For users, the cloud computing industry promises tremendous prospects of market growth, but a wide range of potential risks and safety issues remain prominent [16]. Cloud challenges ranges from data privacy issues, responsibilities for security breach, loss of physical control, availability concerns, cloud data backup and recovery, implications for e-discovery, compromised system security, inaccurate billing, greater dependency on third parties, to the inability of enterprises to satisfy audit/assurance charter and requirements of regulators or external auditors [1], [2], [18]. Well known incidents with cloud services include: Amazon's EC2 cloud service partial outage, the security breaches of Sony's PlayStation Network and Qriocity music service [19]. These events emphasized that customers' inability to control their data remains a key issue of the cloud computing model [19].

The Institute of Internal Auditors indicated that today's auditors are faced with increasingly new-and-improved technologies (including cloud computing) that are transforming the business environment but introduces new risks that must be managed [11]. Hence, through this research, an SLA evaluation template aimed at cloud computing services, based on the COBIT 5 for Risk framework was developed.

(a) Cloud Computing Defined.

According to the National Institute of Standards and Technology (NIST) and Cloud Security Alliance (CSA), *"Cloud computing is a model for enabling 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"*. Cloud is composed of five essential characteristics, three service models, and four deployment models [20, 21].

1.2 Problems with Cloud SLAs

Gartner's 2010 EXP Worldwide Survey of nearly 1,600 Chief Information Officers, indicates that spending on IT cloud services is expected to grow almost threefold over the next five years [14]. Although cloud computing has evolved as a business solution, there are significant associated risks that must be addressed. As enterprises implement this technology, the integration and alignment of the services delivered by the Cloud Service Provider (CSP) remains an ongoing priority.

1.3 Research Questions and Scope

This research attempts to answer these cloud related questions and concerns:

- How can potential cloud users effectively evaluate and select the best suitable CSP for their business needs while minimizing potential risks (what standard or reference SLA parameters can be used to measure CSP's performance)?

- How can cloud users rely on cloud providers to secure and protect their data and information assets (what assurance do cloud users have about cloud services and who will provide this assurance)?

2. Discussion and Analysis

2.1 Literature Review

The related works reviewed are categorized into: Cloud Governance, Cloud Computing Market Maturity, Service level agreements (SLAs), as well as Security, Compliance and Data Privacy. The various categories are discussed in subsequent sections.

(a) Cloud Governance

According to Gartner, good governance practices, the ability to choose a suitable cloud computing environment, as well as security and privacy are the key challenges in cloud computing[2]. Boards of Directors are advised to guide the cloud investments to ensure optimization of risk, control of associated costs and creation of enterprise value [15].

Jirasek highlighted the importance of establishing and enforcing good governance practices for cloud computing projects [5]. To realize strategic, economic and operational benefits from cloud computing, enterprise goals and objectives must be aligned with adoption drivers [3]. Flexibility, reduced initial investment cost, faster deployment and virtualization are some of the cloud characteristics that may demand more governance considerations so that benefits are realized within the enterprise's risk appetite [3]. The enterprise's ability to buy only what it uses was reinforced as one of the goals of cloud computing [3]. ISACA advised focusing on using competition among cloud service providers as a bargaining chip to negotiate the best prices since the core can be provisioned and modified as needed [3].

According to ISACA, in order to discern whether cloud services will meet board's expectations, there should be an initial alignment between the enterprise strategy and expectations [3]. For effective cloud governance, the establishment of a mutual understanding of expected benefits, as well as tracking and measuring tools should be prioritized [3]. ISACA proposed COBIT 5 as a tool for governing and managing cloud investments, in addition to implementing consistent practices to maximize value and control risk [3]. Hence, it is evident that governance is a key area in cloud computing that helps ensure alignment with business strategy and priorities. Thus, the importance of SLA management in the governance framework cannot be overemphasized.

(b) Cloud Computing Market Maturity

Although cloud computing is still in its early stages of maturity, significant concerns will continue to be addressed [6, 7]. Cloud computing should be seen more as a business enabler and less as a technology issue so that the technology can progress in its maturity levels and enterprises can derive promised benefits [7].

The need for executive management to gain an understanding and appreciation for cloud by seeing it as a source of innovation was also highlighted [7]. Furthermore,

[2] http://www.gartner.com/technology/topics/cloud-computing.jsp

cloud risks should be addressed at the enterprise level rather than as a technical issue [7]. Hence, to ensure cloud computing progresses through its maturity levels and benefits are maximized, an enterprise should address risk areas like security, privacy, data ownership, etc. These can be negotiated with the provider through SLAs.

(c) Security, Compliance and Data Privacy

According to Awad, cloud computing is best implemented through a phased-in approach [10]. Security, application type to be transitioned, as well as the CSP's proven track record, financial stability, and allowance for negotiating suitable terms are the key considerable factors in selecting the right cloud partner [10].

Long-term viability, privileged user access, data segregation, recovery, vulnerability to attack or breaches, and regulatory compliance were also among customers' security concerns listed [8]. Jurisdictional issues, whereby the cloud user needs to comply with both laws governing its own country and that of the country where its data is stored was highlighted [8]. Where there is a conflict of laws, further consideration should be given to security levels at the physical location where cloud services will be deployed and managed [8]. Since cloud providers are required to physically separate backup data from production data, location of the offsite backup data becomes a compliance issue as it could be stored outside the client's legal/regulatory jurisdictions. While vendors may not disclose city, state, or country the backup data is stored, they should be willing to work with the client to provide, and prove compliance of the offsite backup data location [17].

A survey of IT executives by IDC eXchange, highlighted that security, availability and performance[3] are key challenges facing cloud services. The work done by Symantec to help enterprises make the right decisions in evaluating CSPs affirmed that security, compliance and data privacy remain areas of concern when considering the use of cloud services [12]. This paper focused on how CSPs could leverage secure sockets layer (SSL) certificates to deliver desired security levels for enterprises. Gartner Research identified seven areas of security risk associated with cloud computing that should be evaluated by enterprises when selecting a cloud hosting provider: privileged user access, compliance, data location, data segregation, recovery, investigative support and viability [13].

For secure and confidential data, enterprises are under regulations. Outsourcing services to CSPs does not relinquish consumer's responsibility for compliance. As due diligence, cloud users should ensure CSPs are preventing unauthorized third-party access or modification to address compliance risks [12]. As an added layer of protection, SSL deployed in backup and recovery ensures that backup data accessed is encrypted in transit, and servers accessed for backup data are authenticated as legitimate sources [12]. SSL is the proven technology for cloud security as it helps in developing trust between cloud user and provider [12].

According to Wei, Murugesan, Kuo, Naik and Krizanc, CSPs must implement strategies that enhance data integrity and privacy to address users' security concerns [24]. New data auditing and encryption techniques to protect cloud users' data from

[3] http://blogs.idc.com/ie/?p=730

cyber-attacks while assuring a high level of data availability were also proposed [24]. Hence, addressing security and compliance issues in SLAs remain paramount.

(d) SLAs

According to Gartner, establishing the right SLA prior to the cloud user-vendor relationship is essential [14]. In a survey, CSA and ISACA affirmed that SLAs form the basis for clear definition and enforcement of user expectations, in addition to adequately documenting expectations of what the cloud provider will offer [7]. Based on related work, different but overlapping components or concerns to be addressed in an SLA are summarized in Table 1.

Table 1. Summary of Existing Work Related to SLA Components

SLA Component	References
Business requirements for availability, response time for incidents and additional computing resources, change and patch management.	[1], [4], [7], [9].
Provisions for disaster recovery, business continuity and physical access controls.	[4], [8], [9], [13], [14].
Penalties for non-compliance to SLAs	[1], [14].
SLAs for security (Sec-SLAs)	[8].
CSP and cloud user's responsibilities for data and security, alignment of security metrics with industry standards and practices.	[4], [8], [9], [14].
Confidentiality agreement, exit strategies, and portability (moving from one CSP to another).	[1], [9], [13].
Data retention and disposal policies and procedures	[4], [13].
Controls to satisfy legal, compliance and jurisdictional requirements.	[4], [8], [13], [24].
Monitoring and performance measurements	[1], [8].

Therefore, inadequately defined SLAs contribute to a risky relationship between the cloud user and service provider [7]. As more enterprises leverage cloud computing, some of the service providers are offering competitive prices while others are being distinguished by quality of service through availability, and enhanced security.

2.2 Research Methodology

An initial comprehensive search for existing cloud SLA evaluation templates was carried out. Next, a list of the ten most important cloud computing companies was looked at, but the top five CSPs were critically compared, as well as their respective SLAs: Amazon, VMware, Microsoft, Salesforce and Google [25]. Public cloud vendors (Amazon, Microsoft and Google) were asked questions related to the infrastructure and platform services as suggested by cloud analysts and consultants [26]. Note that at the time of this research, Amazon had created a unique niche market where their larger cloud consumers are given the opportunity to customize cloud SLAs, thereby defining terms that best meet their business needs. The comparison is

summarized in Table 2 and this is not conclusive due to rapid change of CSP offerings.

The study and analysis by Cloud Spectator compared five large cloud IaaS providers (Amazon, Rackspace, HP Cloud, SoftLayer and Windows) to determine their price-performance value, and Microsoft Windows topped the list in terms of customer satisfaction (performance) [27].

Table 2. Top 5 SLAs Analysis - Side by Side Comparison

	Amazon	*VMware*	*Microsoft*	*Salesforce*	*Google*
Availability/ Uptime Guarantee	99.95%	99.9%	99.95%	N/A	99.95%
Custom cloud SLA	Yes	N/A	No	N/A	No
Compensation for downtime	Service credit	Service credit	Service credit	N/A	Service credit
Reporting uptime	Public dashboard	N/A	Public dashboard	N/A	Public dashboard
Publicly post audits	Limited	N/A	Limited	N/A	Limited
Audits of controls by customers/ potential customers	No	N/A	No	N/A	No
Customer-led penetration testing (simulate cyber-attack)	Yes	N/A	Yes	N/A	No
Response-time to notify customers of breach	Based on applicable law	N/A	Promptly	N/A	Per contractual terms
Customers choose cloud storage location	Yes	N/A	Yes	N/A	Yes

(a) Findings and Results

Cloud SLA concepts adapted from NIST, SLA terms and parameters from ISACA and CSA were used to formulate a scorecard prototype of SLA components that should be negotiated and documented in cloud SLAs [4], [21], [22]. According to Tschinkel, security in addition to data privacy and availability concerns are to be addressed as these are some of the most critical areas of risk management for the cloud [17]. A vendor market survey was carried out to justify the selection of cloud providers and at the time of research, Amazon and Microsoft emerged at the top for the following reasons: customization of cloud SLAs and customer satisfaction. Hence, these best practice SLA terms were grouped in five areas, though some are applicable in more than one area: Confidentiality, Integrity, Availability, Auditability and Customer Satisfaction. Case in point is the ‘Interoperability and Portability’ component that fits into Integrity and Customer Satisfaction.

Patel, Ranabahu and Sheth proposed the Web Service Level Agreement (WSLA) framework as a mechanism for managing SLAs in a cloud computing environment, in addition to being developed for SLA monitoring and enforcement in a Service Oriented Architecture (SOA) [23]. The third party support feature of WSLA was used to delegate monitoring and enforcement tasks, in addition to presenting a real world use case to validate their proposal [23]. However, a risk-based approach in alignment with COBIT 5 for Risk was not adapted or mentioned.

At the time of research, no existing cloud computing SLA evaluation template aligned with the COBIT 5 for Risk framework was found. So, these key SLA terms were mapped to COBIT 5 for Risk and the resultant scorecard prototype was used to test Amazon's SLA.

The scorecard prototype becomes the basis of risk analysis for the IT Risk Scenarios in COBIT 5 for Risk framework for cloud SLAs. An IT Risk scenario is an event that can lead to loss and has a business impact, when and if it occurs [28]. These IT Scenarios were adapted to the cloud environment and embedded into the gap analysis.

Table 3. Testing the Scorecard Prototype (SLA Components) based on best practices from NIST, ISACA and CSA with Amazon's SLA

Scorecard Prototype		**Amazon Elastic Compute Cloud (Amazon EC2) SLA**		
SLA Components		***Addressed***	***Not Addressed***	***Vague***
Confidentiality	SSL, Encryption based on data classification (data at rest and in transit), Data (Information) Dispersion, Secure Disposal (data security lifecycle), User Management, Access Control/Authorization, Human Resources/NDAs, Identity and Access Management, Segregation of Duties (SoD), Third Party Access, Security controls.		√ √ √ √ √ √ √ √ √	
Integrity	Interoperability and Portability - must not affect data in any way, Data segregation (per multi-tenancy).		√ √	
Availability	Uptime, Contingency Planning (IR, DR, BC), Data Retention, Backup and Recovery, Response time, Source code escrow.	 √	 √ √ √	 √
Auditability	Independent Audits; sub-categories: Type of audit (type I or II), Frequency (annual/semi-annual), scope/quality (is CIA covered), credibility/reputation of the auditing firm, Change Management, Configuration Management and Patch Management, Audit Logging and Monitoring, Penalty for noncompliance, Cross-border issues /Compliance with Jurisdictional laws on Data Location, Security breach disclosure responsibilities, Third party certification (ISO/IEC 27001/27017, SAS 70, PCI, etc.): sub-categories-Type, Frequency and CIA Components should be part of the report, System of internal controls (e.g. Policies and Procedures), Review of SLA metrics and compliance, Right to audit clause.	 √	 √ √ √ √ √ √ √ √	 √
Customer Satisfaction (UnixBench components)	Pricing Plans, Performance (usage, load balancing, delivery, quality, etc.), Maintenance and Service Support, Flexibility to Customers' Request, Scale Up/Scale Out - Interoperability and Portability.	 √ √	√ √ √	

Table 4 shows the mapping of the SLA components to COBIT 5 for Risk. The complete analysis table shows the twenty example scenarios that were adapted from COBIT 5 for Risk and tailored to cloud computing. These Risk Scenario Categories are high level descriptions of the category, while Risk Type are types to which scenarios derived from the gap analysis will fit (using three risk types which could be primary fit (higher degree)-P/secondary fit (lower degree)-S/blank for non-related risk scenario). The three risk types are [28]:

- *IT benefit/value enablement risk* (resulting from lost opportunities to leverage technology for new business initiatives or improve the efficiency or effectiveness of business processes).
- *IT programme and project delivery risk* (related to the contribution of IT to new or improved business solutions, through projects and programmes).
- *IT operations and service delivery risk* (as a result of operational stability, availability, protection and recoverability of IT services that can destroy or reduce enterprise value).

Table 4. Mapping of SLA Components to COBIT 5 for Risk - Cloud SLA Evaluation Template

Risk Scenarios based on COBIT 5 for Risk						
		Risk Type (P/S)				
#	***Risk Scenario Category***	***IT Benefit/Value Enablement***	***IT Programand Project Delivery***	***IT Operations and Service Delivery***	***SLA Components from Table 3***	***Example scenarios***
1	Portfolio Establishment and Maintenance	P	P	S	N/A	Ensure selected cloud services are aligned with business strategy and priorities. Prior to adoption, cloud services should be assessed for compatibility with existing architecture.
2	Program/projects life cycle management (program/projects initiation, economics, delivery, quality and termination)	P	P	S	Performance (usage, load balancing, delivery, quality, etc.) Change management Maintenance and Service Support	Cloud projects are within scope, allocated budgets and delivered on time without deteriorating quality. Stakeholders are actively involved from initiation to the end to avoid failure. Change management is deployed to keep stakeholders informed and future users trained.
3	IT investment decision making	P		P	N/A	There's alignment between business and IT when making cloud investment decisions. Business case is drawn up to justify cloud investments.

4	IT expertise and skills	P	P	P	Human Resources/ NDAs User Management, Access Control/ Authorization Identity and Access Management, SoD Third Party Access	Due diligence and screening of candidates involved either at the cloud consumer's end or vender's to ensure appropriate skills and competences in the recruitment process. Security education, training and awareness (SETA) to ensure staff are up to date with the latest cloud developments. Segregation of duties and job rotation to ensure no single employee knows the entire system. Suitable staff with appropriate skills and competences are attracted to support business objectives, service and value delivery. Staff and 3rd party access or authorization is granted based on Least Privilege and Need-to-Know principles.
5	Staff operations (human error and malicious intent)	P	S	P	Configuration, Patch, Identity and Access Management, Uptime, Contingency Planning (IR, DR, BC), Backup and Recovery Response time, System of internal controls, Security controls Logging and Monitoring	Configuration management is leveraged to elude errors. Avoid authorization creep so that access rights from prior roles are not abused. Coordination between HR and IT Administration to ensure timely removal of access rights to deter abuse. For security, two separate individuals should approve before actions are taken (the 4-eye principle) especially in the areas of backup, information entry, system maintenance and upgrades. Data centre is secured, monitored for irregularities and only authorized staff are granted access. Ensure appropriate security controls are in place to deter theft. Ensure monitoring for performance, availability and other irregularities, in addition to prompt response to alerts.

6	Information (data breach: damage, leakage and access)	P	S	P	SSL, Encryption based on data classification (data at rest and in transit) Data (Information) Dispersion Secure Disposal (data security lifecycle) Data Retention, Data segregation (per multi-tenancy) NDAs Contingency Planning (IR, DR, BC), Backup and Recovery Security breach disclosure responsibilities	Contingency planning to ensure that if database is corrupted or hardware components are damaged, data would be available. Backup procedures based on data classification levels are in place, in addition to testing backups and protecting backup media. Through continuous network monitoring and firewalls, sensitive information on cloud provider or consumer's site is protected. SETA to ensure staff do not accidentally disclose sensitive information through social media or email. To protect data, portable media are secured and encrypted. Intentional modification of information is prevented through the 4-eye principle. Regular update of the data retention policy to avoid inefficient archiving, retaining or disposal of information. Non-disclosure agreements and intellectual property clauses are factored into contracts to avoid leakage information or trade secrets and loss of competitive advantage.
7	Architecture (architectural vision and design)	P	S	P	Scale Up/Scale Out	Cloud consumer's architecture should be flexible to support adoption of newly acquired cloud services in a timely manner.
8	Infrastructure (hardware, operating system and controlling technology) (selection/implementation, operations and decommissioning)	P	S	P	Scale Up/Scale Out Performance (usage, load balancing, delivery, quality, etc.)	Newly acquired cloud services should not make consumer's systems unstable leading to operational incidents. Underlying infrastructure should allow for scale up/scale out in case user volumes increase or handle system load when new cloud services are deployed. Cloud services should be tested prior to deployment into the production environment to ensure system availability and proper functionality. Hardware and utilities should be protected from failures, in addition to putting standby measures in place to support continual execution of critical business transactions.

9	Software	P		S	Source code escrow Change and configuration Management Backup and Recovery	For SaaS models, contingency planning should include source code and data escrow to assure business continuity regardless of what happens to the SaaS provider. SaaS customers could enter into an agreement with the 3rd party hosting provider to continue hosting the application in case the SaaS vendor goes out of business. Change control and change management should be in place to reduce incident resolution time and problem management. Roll-back procedures are in place in case of operational issues, in addition to establishment of backup and restore points in accordance with business needs.
10	Business ownership of IT	P	S	S	Review of SLA metrics and compliance	Cloud initiatives should not be a sole responsibility of the technical team, enterprises should assume accountability to ensure alignment with business strategy. Business requirements should be adequately defined and reviewed to ensure effective SLAs. Cloud investments are within the procurement process and weighed based on cost vs. benefits.
11	Supplier selection/ performance, contractual compliance, termination of service and transfer		S	P	Review of SLA metrics and compliance Performance (usage, load balancing, delivery, quality, etc.) Maintenance and Service Support, Flexibility to Customers' Request, Penalty for non-compliance, Interoperability and Portability	Prior to a strategic partnership, enterprises should exercise due diligence in selecting the CSP; check the financial viability, delivery capability, as well as sustainability of the CSP. Cloud services and support should be reviewed to ensure they're in accordance with the SLA. Defined key performance indicators (KPIs) should be linked to rewards and penalties to ensure adequate service delivery and support. If the partnership ceases to exist, there should be measures that allow for interoperability and portability (exit strategies). To avoid service integration issues with existing services, the enterprise should consult/involve IT before purchasing cloud services.
12	Regulatory compliance	P	S	P	Independent Audits, Credibility/reputation of the auditing firm, Third party certification, Review of SLA metrics and compliance Right to audit clause, Cross-border issues/ Compliance with Jurisdictional laws on Data Location	Independent audits and 3rd party certification should be carried out to assure compliance with regulatory standards. The consumer can request for a right to audit clause in contractual agreements and ensure the CSP is willing to work with the consumer to comply with regulations that prohibit cross-border dataflow.

13	Geopolitical			P	Cross-border issues/ Compliance with Jurisdictional laws on Data Location	Ensure that compliance to national, support of local initiatives and government interference does not affect the partnership between cloud consumers and their service providers, in addition to service capabilities.
14	Infrastructure theft or Destruction	S	S	P	Contingency Planning (IR, DR, BC) Security controls Logging and Monitoring	Security controls and contingency planning should address theft of servers or devices with sensitive data, in addition to destruction or sabotage of data centres. Access to data centres should be logged, monitored and restricted only to authorized personnel.
15	Malware	S		P	Contingency Planning (IR, DR, BC) Security controls Logging and Monitoring	Through firewalls, security controls, contingency planning and continuous monitoring of network, cloud infrastructure should be protected against malware, logical bombs, and loss of data through phishing attacks.
16	Logical attacks	S		P	Contingency Planning (IR, DR, BC), Security controls Logging and Monitoring Identity and Access Management	Through firewalls, security controls, contingency planning and continuous monitoring of network, cloud infrastructure should be protected against hacking, unauthorized access to systems, industrial espionage and service interruption due to denial-of-service attacks.
17	Industrial action	S	S	P	Contingency Planning (IR, DR, BC)	Through contingency planning, alternate solutions where critical business tasks can be executed should be planned for in case the 3rd party or primary location becomes unavailable due to strike.
18	Environmental	S	S	P	Contingency Planning (IR, DR, BC)	Ensure that equipment used at data centres is environmentally friendly (e.g., power consumption).
19	Acts of nature	S	S	P	Contingency Planning (IR, DR, BC)	Contingency planning should take into consideration the impact of natural disasters on cloud services, if and when they occur.
20	Innovation	P		S	Security controls Pricing plans	New and important technology trends in cloud computing that have been identified should be timely assessed for business impact and adopted if required. The security controls and cost of the new trends should be considered.

Amazon's publicly available SLA - Elastic Compute Cloud (Amazon EC2) was tested against the scorecard prototype and results are shown in Table 3 above. The rating scale in three categories are: Addressed (where the SLA component is clearly stated), Not Addressed (if not stated) and Vague (if it's unclear how the SLA compo-

nent is addressed). According to the test, majority of the SLA components fall into the 'Not Addressed' category and are gaps to be discussed or negotiated with the CSP. This is just an example of how the scorecard prototype can be applied to any SLA.

This initial audit helps in identifying gaps and risks the enterprise needs to manage. If an SLA component is not stated in the SLA, it becomes the customer's responsibility. Where the SLA component is important, the cloud consumer should see if it can be negotiated with the CSP to reduce risk and cost. The importance of evaluating the amount of risk being shared cannot be overemphasized. This evaluation should also identify the risk either the consumer or CSP are responsible for. Any risk that cannot be negotiated with the CSP must be addressed by the consumer through various risk management practices. The goal is to realize benefits from cloud initiatives while optimizing resources and managing risks.

3. Conclusion

In this paper, a scorecard prototype was developed to effectively help cloud users evaluate and select the best suitable CSP for its business needs while minimizing potential risks. Best practices from NIST, ISACA and CSA were identified as reference SLA parameters that can be used in SLAs and measurement of provider's performance. Incorporating these terms in SLAs (either as standard or negotiated terms), assures cloud users of their providers' commitment and responsibility in securing and protecting their data, as well as information assets.

Though the initial evaluation template has been generalized, this paper is the first in its direction for future work where each SLA component can be further addressed. Recommendations for future work also includes taking a company considering moving to the cloud as a case study, specifically tailoring the template for the company, and testing the template prior to acquiring cloud services.

Acknowledgement

The first author will like to thank Concordia University of Edmonton's research team for their guidance and support in the completion of this work. Their efforts, knowledge and experience were instrumental in making this paper a success. She acknowledges the Academic Research Council for the Student Research Grant awarded to her. She is also thankful to God Almighty, her family and friends; this has been a journey and she is very grateful for their love, support and encouragement.

References

1. Information Systems Audit and Control [ISACA]: Cloud computing management audit/assurance program (2010)
2. Gadia, S.: Cloud computing: an auditor's perspective. ISACA Journal (2010)
3. ISACA: Cloud governance: questions boards of directors need to ask (2013)
4. ISACA: Security considerations for cloud computing (2012)
5. Jirasek, V.: Cloud governance done right: examples from the trenches. BrightTALK (2013)

6. Sinnett, W.M: In the Cloud and Beyond. Financial Executive (February 2012)
7. CSA and ISACA: Cloud computing market maturity: study results (2012)
8. de Chaves, S. A., Westphall, C.B., Lamin, F.R.: SLA perspective in security management for cloud computing. In: IEEE ICNS, pp. 212 - 217 (2010)
9. Subbiah, S., Muthukumaran, S.S., Ramkumar, T.: Enhanced survey and proposal to secure the data in cloud computing environment. In: IJEST Vol. 5 No.01 (2013)
10. Awad, R.: Considerations on Cloud Computing for CPAs. In: The CPA Journal, Vol. 81, No. 9 (2011)
11. Jackson R.A.: Audit in a digital business world. In: The Internal Auditor Magazine, pp. 36-41 (August 2013)
12. Symantec Corporation: Choosing a cloud hosting provider with confidence: Symantec SSL certificates provide a secure bridge to trusted cloud hosting providers (2012)
13. Heiser J., Nicolett, M.: Assessing the security risks of cloud computing. Gartner Research, ID G00157782 (2008)
14. Smith, D.M, Plummer, D.C, Bittman, T.J, Bova, T, Basso, M, Lheureux, B.J, Prentice, B.: Predicts 2013: Cloud computing becomes an integral part of IT. Gartner, ID: G00230929 (December 2012)
15. Gartner, http://www.gartner.com/technology/topics/cloud-computing.jsp
16. Wu, J., Shen, Q., Wang, T., Zhu, J., Zhang, J.: Recent advances in cloud security. In: Journal of Computers, Vol. 6, No. 10 (2011)
17. Tschinkel, B.: Cloud computing security understanding risk areas and management techniques (2011)
18. Gordon, M.: The compliant cloud. BrightTALK (2009)
19. Moore, J. [CNBC]: Reducing security risks in cloud computing, http://www.cnbc.com/id/43139361/Reducing_Security_Risks_in_Cloud_Computing
20. Badger, L., Grance, T., Patt-Corner, R., Voas. J.: Cloud computing synopsis and recommendations. In: NIST, Special Publication (SP) 800-146 (2011)
21. CSA: Security guidance for critical areas of focus in cloud computing v3.0 (2011)
22. NIST: NIST US government cloud computing technology roadmap, Release 1.0 (Draft) - In: NIST, Special Publication (SP) 500-293 (2011)
23. Patel, P., Ranabahu, A., Sheth, A.P.: Service level agreement in cloud computing (2009)
24. Wei, D.S.L., Murugesan, S., Kuo, S., Naik, K., Krizanc, D.: Enhancing data integrity and privacy in the cloud: an agenda. In: IEEE Computer Society, pp. 87 - 90 (2013)
25. Bort, J.: The 10 most important companies in cloud computing. Business Insider (2013)
26. Loftus, T.: Public cloud vendors side by side by side. In: The Wall Street Journal (2013)
27. Cloud Spectator: Cloud server performance: a comparative analysis of 5 large cloud IaaS providers (2013)
28. ISACA: COBIT 5 for Risk framework, pp. 67-74 (2013)