Cloud Computing: Information Security Standards, Compliance and Attestation

Andrzej J. Gapinski, Ph.D.[1]
[1] Pennsylvania State University, USA, ajg2@psu.edu

Abstract– ***Cloud computing organizations as service organizations have to conform to compliance regulations, certifications and standards in delivered services. The area of compliance and certification covers not only Information Security (IS) standards and compliance but also areas such as auditing – Attestation Engagement (AE). The paper reviews current information security standards, compliance & attestation standards for organizations offering cloud computing services.***

Keywords— cloud computing, compliance, standards.

Digital Object Identifier (DOI): http://dx.doi.org/10.18687/LACCEI2015.1.1.065
ISBN: 13 978-0-9822896-8-6
ISSN: 2414-6668

Cloud Computing: Information Security Standards, Compliance and Attestation

Andrzej J. Gapinski, Ph.D.
The Pennsylvania State University, USA, ajg2@psu.edu

Abstract–Cloud computing organizations as service organizations have to conform to compliance regulations, certifications and standards in delivered services. The area of compliance and certification covers not only Information Security (IS) standards and compliance but also areas such as auditing – Attestation Engagement (AE). The paper reviews current information security standards, compliance & attestation standards for organizations offering cloud computing services.

Keywords—cloud computing, compliance, standards.

I. Introduction – Cloud Computing

Cloud computing is increasingly being offered by a variety of companies. The services are used for multiple reasons: the ability to reduce legacy costs, the ability to remove maintenance costs, economics of scale, speed and agility, global access & reach. According to Kauffman [1] cloud computing "originates from the telecommunications world of the 1990s, when providers began using virtual private network (VPN) services for data communication. VPNs maintained the same bandwidth as fixed networks with considerably less cost: these networks supported dynamic routing, which allowed for a balanced utilization across the network and an increase in bandwidth efficiency, and led to the coining of the term 'telecom cloud.'" Historically speaking, the companies which offered online data hosting or computing/processing performed at their server based computer facilities were prime candidates to extend the services to cloud computing. The industry is relatively new but already has many established players such as Amazon and Microsoft, among others. In the case of Amazon, Amazon Web Services (AWS) [2,3], the company already had vast data centres in place to host massive amounts of data for their customers. So it came quite naturally to extend the services to offer hosting data for companies. Increasingly, a cloud computing offers online processing where clients access various software with usage fees. Microsoft [4], with its Azure, started to offer cloud processing more recently. Other major companies such as Amazon [2,3], Google [5], EMC [6], and IBM [7] joined the list of companies which offer various online or mobile cloud computing and/or processing.

According to the National Institute of Standards and Technology (NIST) [8] cloud computing is defined as "…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. This cloud model promotes availability and is composed of five essential characteristics: On-demand self-service, Broadband network access, Resource pooling, Rapid elasticity, Measured Service."

Cloud computing as a new information technology platform still evades clear definition and consequently provides some confusion over what it is and what it is not. Kushida et al. [9] in analysing cloud computing in the context of implications for public policies argue to consider cloud computing as "dynamically configured utility." Kushida et al. [9] provide a comparative analysis among above mentioned cloud computing providers such as Amazon, Microsoft, Google, etc., with respect to differences in technology infrastructures and development path.

Major cloud service providers are not bound by specific physical location and offer their datacenters across the world. Thus it is useful to remember about possible classification of cloud services based on "host" location with ramification to legal issues. Namely, cloud computing depending on the location of the host of cervices can be classified into the following categories [10] or modalities [9]: a private, a public, a community-based or a hybrid model.

Cloud services may include:

- Deployment and management of data and processing,
- Mobile services,
- Enterprise applications, or
- Integration with on-premises Resources.

Next we consider standards and compliance regulations with regard to information security, business practices and auditing that cloud service organizations must adhere to.

II. Cloud computing: Information Security, Compliance, Certifications and Attestation Standards

In order to provide customers with assurances about information security and sound business practices, cloud computing service organizations seek certifications and assessment by external agencies in mainly three areas:

- Information Security,
- Compliance with regulations, and
- Attestation / Auditing.

A. Information Security & Compliance

Cloud computing information security and compliance conform to standards used by computer and computer network industry. Schou and Shoemaker [11] and Solomon and Chaplle

[12] provided good background information regarding information assurance and security. Concepts of confidentiality, integrity and availability (CIA) are understood as defined in [12]:

- Confidentiality, or secrecy – the concealment of information
- Integrity – trustworthiness of information or data/resources; ensuring that data can be modified only through an authorized mechanism
- Availability – allowing authorized entities access to assets.

Soo Hoo [13] formulated the comprehensive computer security risk model, which addressed shortcomings of previous modelling schemes. While it combined both deterministic and probabilistic approaches of previous models and thus eliminated inadequacies of its predecessors, an extensive complexity rendered it not applicable especially for small and medium size companies.

Gapinski [14] analysed computer network security in the context of strategies or policies employed by companies. Furthermore, Gapinski [14] defined various levels of trust among network entities which can be helpful in establishing the right security policies and implementable methods for companies.

Naturally clients seeking cloud computing/services are concerned about data security and this concern has the highest priority in their mind. So it does not come as a surprise that security concern is the key inhibitor to cloud computing. In order to ensure that cloud systems provide the desired security, according to [15] one "must first properly plan and assess the environment before migration. It is important to first understand:

- On what type of cloud your service will be hosted.
- How that cloud will be accessed.
- Your company's security and privacy requirements.
- How your company will maintain accountability over the privacy and security of data and applications implemented and deployed.
- Data location.
- Monitoring ongoing assessment and authorization.
- Security incident management."

According to Kauffman [1] the companies which offer services to ensure data confidentiality, integrity, and availability (CIA), must offer capabilities that, at a minimum, include:

- "a tested encryption schema to ensure that the shared storage environment safeguards all data,
- stringent access controls to prevent unauthorized access to the data,
- scheduled data backup and safe storage of the backup media."

Cloud computing companies offer various types of services with different levels of security. Not understanding the offered services and especially the various levels of security provided may lead to security breaches. In addition, the co-existence of public, private, community-based, and hybrid clouds may create additional vulnerabilities. Thus, when the company migrates to cloud processing / computing centres outsourcing some of the functions puts new responsibilities on IT personnel to ensure seamless migration of services.

Data security is an increasingly important concern due to cybercrime. Bloomberg Business Week [16] reports that "cybercrime is already costing the global economy more than $400 billion annually." The U.S. government is considering a cyber-security bill to address the new vulnerabilities [16].

There are a variety of compliance standards in the area of information security and cloud computing that service organization offering cloud storage & computing need to follow. Federal agencies, international agencies, professional organization, and various associations are involved in the formulation, certification, and writing the guidelines.

Cloud services organizations offer services across the world. Legally speaking information and data security host physical location dictates what set of policies and regulations have to be followed. So all legal issues related to information privacy, security, and jurisdiction are specific state bound. In the US, according to the Patriot Act [17] "allows the US government to demand disclosure of any data stored in any datacenter, anywhere in the world if that system is operated by a US-based company" [9]. That law may place American companies at great disadvantage in foreign markets especially when data present vital importance from security or competitiveness point of view. Other recently enacted act such as the Sarbanes-Oxley Act [18] provides a number of reporting requirements for internal controls and reporting procedures [9].

As far as international landscape is concerned, Europe provides a challenging regulatory environment with rigorous data security and privacy regulations. In addition, there are significant regulatory differences among various European states [9]. Legal issues related to international jurisdiction and responsibility have yet to be addressed and resolved [9]. Which rules do apply - of the country where services were consumed or where services did originate? Kushida et al. [9] gives example of Microsoft datacenter in Singapore without a clear answer.

There is a variety of international and other not mentioned above federal standards which apply to information security and data privacy – the most important ones are listed and described below:

- ISO / IEC 27001 International Organizational for Standardizations ISO 27001 [19]. The standard provides requirements for information security management system (ISMS) to ensure security of assets such as financial information, intellectual property, etc.

- PCI DSS – Payment Card Industry Data Security Standard [20]. The standard consists of policies and procedures which optimize the security of credit card transactions and personal data. This standard specifies six requirements which must be satisfied:
  1. secure network (authentication, firewalls, etc.),
  2. secure customer information (encryption of data),
  3. prevention of malicious access (anti-spyware, anti-malware),
  4. restricted access to information, and
  5. network monitoring
  6. information security policy defined, maintained, and followed.
- FISMA - Federal Information Security Management Act [21]. Standards & guidelines for minimum security controls for information systems.
- HIPPA - Health Insurance Portability and Accountability Act [22]. The primary objective is to protect confidentiality and security of healthcare information.
- HITECH – Health Information Technology for Economic and Clinical Health Act [23]. The act prohibits disclosing health data to third party without specific business agreements & security requirements.
- FedRAMP - Federal Risk and Authorization Management Program [24]. This program provides a standard approach for conducting security assessment of cloud systems based on accepted security procedures across the federal government.

B. Assurance / Attestation Engagements

Companies offering cloud computing may seek reporting from the American Institute of CPA [25] which offers Service Organization Controls (SOC) reports. The reports are supposed to help service organizations build trust and confidence of customers in their service delivery processes and controls. There are various types of SOC reports:

- SOC 1 Report on controls at service organization regarding financial statement prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16. Stakeholders: entities which use service organizations, user' auditors, etc. Use is restricted.
- SOC 2 Report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy. The report is planned to meet the needs of users that need information and assurance about controls at service organizations that affect the security, availability, and processing integrity of systems used by service organizations. Stakeholders may include: management of service organization, regulators, customers, etc. Use is restricted.
- SOC 3 Report on trust services. The report is designed to meet the needs of users who need assurance about the controls at a service organization that affect the security, availability, confidentiality/privacy, and processing integrity of the systems used by a service organization. Freely distributed to all interested parties.

The summary which may help to identify the needed SOC report is listed in Table 1 after [25].

TABLE I
SOC TYPES

How to Identify the SOC Report that is Right for You?		
Question	Yes/No	Recommended Report Type
Will the report be used by your customers and their auditors to plan and perform an audit or integrated audit of your customer's financial statements?	Yes	SOC 1 Report
Will the report be used by your customers as part of their compliance with the Sarbanes-Oxley Act or similar law or regulation?	Yes	SOC 1 Report
Will the report be used by your customers or stakeholders to gain confidence and place trust in a service organization's systems?	Yes	SOC 2 or SOC 3 Report
Do you need to make the report generally available or seal?	Yes	SOC 3 Report
Do your customers have the need for and ability to understand the details of the processing and controls at a service organization, the tests performed by the service auditor and results of those tests?	Yes	SOC 2 Report
	No	SOC 3 Report

There are various attestations standards such as SSAE 16, ISAE 3402 [26] among others, which require SOC1-3 class reporting. The service companies who operate globally offering various cloud computing/processing services may seek an assurance report from International Standards for Assurance Engagements (ISAE) No. 3402 [26].

CONCLUSIONS

Due to its use of the Internet, cloud computing brought renewed interest in certifications and compliance with regard to information security standards, compliance with regulations, and auditing norms. Cloud computing service organizations as part of computer & computer network industry must adhere to various standards and be compliant with regulations in information security, their business practices and auditing norms. The purpose of the article was to review information

security, data privacy, and compliance standards as they apply to services offered by cloud computing providers. Since information security is the primary concern of customers, the companies offering cloud computing services seek certifications and proof of adherence to various standards to build confidence and trust of their customers. Naturally, depending on type of cloud computing services being offered and/or requested some of the above described standards and compliance regulations will play more important role than others. One may observe that rich regulatory and compliance standards as related to cloud computing will necessitate from customers to be knowledgeable consumers. Consequently, the importance of information technology officers/managers of customer organizations will rise. As more and more corporations and organization will migrate toward the cloud services the management and IT officers have to take more proactive role in educating themselves with the offerings and limitations of cloud service providers' environment. With the increasing role of cloud computing services to business and industry, the compliance standards, certifications and adherence to state, federal and international regulations and norms should only gain in importance.

REFERENCES

[1] L. M. Kauffman,"Data Security in the World of Cloud Computing," IEEE Computer Society. Issue no. 04 vol. 7, July/August, 2009, pp. 61-64.

[2] J. Varia, S. Mathew. "Overview of Amazon Web Services." https://d36cz9buwru1tt.cloudfront.net/AWS_Overview.pdf. January 2014.

[3] aws.amazon.com

[4] http://azure.microsoft.com/en-us/

[5] https://cloud.google.com

[6] http://www.emc.com/partnerships/service-providers/index.htm

[7] http://www.ibm.com/cloud-computing/us/en/iaas.html

[8] http://csrc.nist.gov/groups/SNS/cloud-computing/

[9] K. Kushida, J. Murray, J. Zysman."Diffusing the Cloud: Cloud Computing and Implications for Public Policy." J Ind Compet Trade. 2011. 11:209-237. DOI 10.1007/s10842-11-0106-5.

[10] http://www.rackspace.com/knowledge_center/whitepaper/understanding-the-cloud-computing-stack-saas-paas-iaas

[11] C. Schou, D. Shoemaker, *Information Assurance for the Enterprise. A Roadmap to Information Security*, McGraw-Hill, New York, 2007.

[12] M.G. Solomon, M. Chapple, *Information Security Illuminated*, Jones & Bartlett Publishers, Sudbary, Massachusetts, 2005.

[13] K.J. Soo Hoo,"How Much Is Enough? A Risk-Management Approach to Computer Security," Consortium for Research on Information Security and Policy (CRISP), Stanford University, 2000.

[14] A. Gapinski,"Strategies for Computer Networks Security," *Enterprise Science Quaterly Journal*, nr 3 (32) July-September 2014. Warsaw School of Economics. Kwartalnik Nauk o Przedsiebiorstwie. Nr 3 (32). Lipiec-Wrzesien, 2014. Pp. 59-65. www.przedsiebiorstwo.waw.pl

[15] http://cloud.cio.gov/action/secure-your-cloud

[16] Bloomberg Business Week. "The Right Way to Fight Cybercrime," February 9-15, 2015.

[17] http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

[18] http://www.sec.gov/about/laws.shtml

[19] www.iso.org

[20] www.pcisecuritystandards.org

[21] http://csrc.nist.gov/groups/SMA/fisma/

[22] http://health.state.tn.us/hipaa/

[23] http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

[24] http://www.gsa.gov/portal/category/102375

[25] www.aicpa.org

[26] www.isae3402.com