Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Selecting a trusted cloud service provider for your SaaS program

Changlong Tang[*], *Jiqiang Liu*

Institute of Information Science, Beijing Jiaotong University, Beijing 100044, China

ARTICLE INFO

Article history:
Received 28 August 2014
Received in revised form
26 December 2014
Accepted 6 February 2015
Available online 19 February 2015

Keywords:
SaaS
Software as a service
Cloud security
Trusted cloud services
Function
Auditability
Governability
Interoperability
Security assurance

ABSTRACT

Software as a Service (SaaS) offers major business and IT benefits that organizations are looking to take advantage of. SaaS adoption presents serious and unique security risks. Moving a company's sensitive data into the hands of cloud providers expands and complicates the risk landscape in which the organization operates.

This paper highlights the significance and ramifications of a structured selection of a Cloud Service Provider (CSP) in achieving the required assurance level based on an organization's specific security posture. This paper proposes a holistic model, known as the Function, Auditability, Governability and Interoperability or FAGI, as an approach to help a Cloud Service Consumer (CSC) to engage and select a trusted CSP through four major decisions: Selecting a safe cloud that has adequate security functions; Choosing an auditable cloud via third-party certifications/assessments or self tests; Picking out a governable cloud that provides the required transparency; Opting for a portable cloud that ensures the desired portability.

A case study reveals the FAGI approach offers an objective and efficient way to choose a qualified and trusted cloud service and in turn saves CSCs' time, effort, and grief.

1. Introduction

Cloud computing is not just a trend anymore. The cloud has changed how enterprises design and deliver applications. This change in application design and delivery has altered where information is stored, how it is accessed, and how it is managed (KMPG, 2011). Organizations are planning to, or have already started, to integrate cloud into their organizations' IT systems due to the extremely compelling cost-saving potential for cloud based deployments (Joyent, 2012). The benefits from cloud (especially SaaS) include: reduced time to value, increased connectivity, lower cost, scalability, integration and ease of use.

The benefits need to be balanced by the potential risks that come from cloud computing. The primary risk comes from the very nature of cloud services: the co-localization of large amounts of valuable data. Criminal attackers can go directly to one source for multiple corporation and users sensitive data rather than attacking multiple networks and users. For the cloud to reach its incredible potential, business cloud customers must address security gaps that represent significant threats, especially to large organizations and those in heavily regulated industries in order to securely realize the full IT and business benefits available.

A whole spectrum of new risks and threats exist in the cloud that were not present on traditional on-premise based

* *Corresponding author*. Unit 301, 115 Cherryhill Blvd. London, ON N6H 2L8, Canada. Tel.: +1 1226 376 5251.
E-mail address: AlanTang.it@gmail.com (C. Tang).
http://dx.doi.org/10.1016/j.cose.2015.02.001
0167-4048/

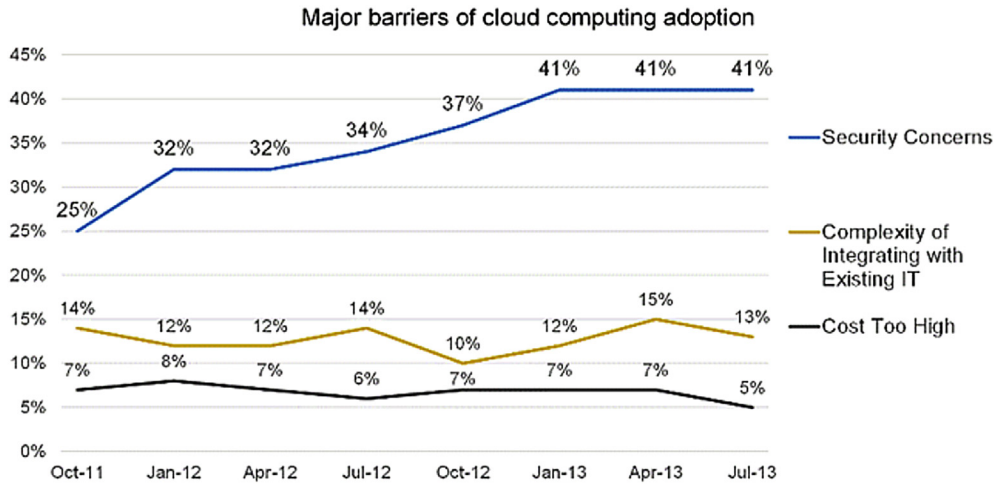

Fig. 1 – Barriers of cloud computing adoption. Note: color on the Web only.

networks. Although the security capabilities for SaaS applications have developed greatly they are still in flux with no standards for individual organizations to build their information security. In many cases, information security has proven to be one of the major barriers to cloud adoption as shown in Fig. 1 (ChangeWave Research, 2013).

The role of the Chief Information Security Officer (CISO) is changing. Traditional responsibilities of securing on-premise infrastructure, applications, people, and processes are moving into hybrid and cloud environments requiring different strategies and techniques. Conventionally, security was seen as a technical requirement of the SaaS program. The ability to protect critical data is becoming a part of business goals and objectives (Dimension Data, 2012).

Understanding the interaction of cloud computing and the regulatory environment is a key component of any cloud strategy. General perceptions around cloud security are an aggregate of specific concerns (HiMSS, 2012). The ability to vet those out may disperse some perceived concerns in lieu of the truth: the cloud can be secure. More and more people are demanding SaaS programs today causing security standards to mature and become commoditized (CloudComputingAdmin, 2014). Also, many organizations do not realize that the cloud does not just bring security

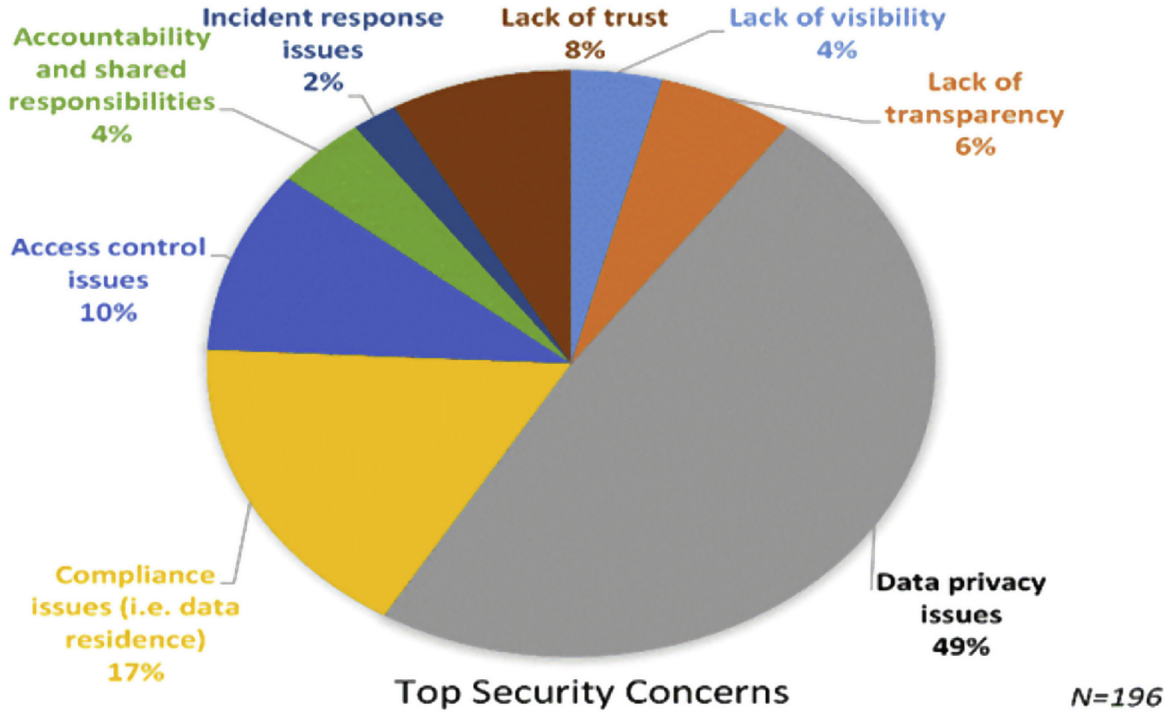

Fig. 2 – Top security concerns of SaaS. Note: color on the web only.

problems, it could also bring potential security advantages such as stronger security capabilities from service providers, especially for small organizations (CCToffice, 2013).

This article will help organizations to take advantage of SaaS programs while controlling and mitigating security risks and concerns. This paper is organized as follows: Section 2 analyses the security challenges in a cloud service realm. Section 3 proposes a FAGI framework and associated processes for security assurance for SaaS. Section 4 introduces a case study to validate the approach by applying the FAGI model to a real project. Section 5 concludes the paper.

2. Key security challenges for SaaS

In order to get a clear picture of major security challenges surround typical SaaS, we collected and analyzed input from both end users and industry experts, as demonstrated below.

2.1. *SaaS user perspective*

We conducted a survey among 196 participants, who were mainly security directors and managers from various industries, during a webinar session. Three questions were polled regarding top concerns, independent validation, and security protections provided from CSPs.

2.1.1. *Top concerns*

As illustrated by Fig. 2, 49% of the respondents indicated data privacy issues are their top concerns. Compliance issues are the second most common concern (17%). The additional six concerns were related to access control, transparency, trust, visibility, responsibilities and incident response.

2.1.2. *Independent validation*

Most organizations do not have the capability or willingness to validate security controls CSPs claim they have. Third-party validation is becoming a viable option in terms of providing some level of verification.

78 percent of people surveyed believed that independent validation/certification/audit is a good approach to provide a certain level of trust between clients and service providers, as stated in Fig. 3.

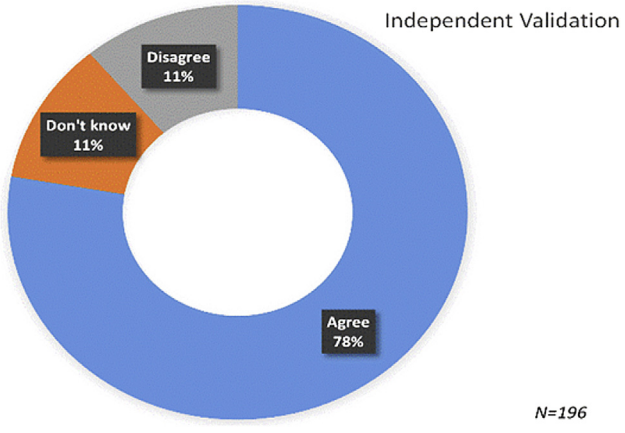

Fig. 3 – Independent validation. Note: color on the web only.

2.1.3. *Security controls from CSPs*

As illustrated in Fig. 4, 48 percent of respondents thought cloud service providers (e.g. Amazon, Google and Microsoft) provide improved security protections and compliance controls that some organizations otherwise could not provide as efficiently or effectively themselves. As more and more SaaS vendors come online, competition will ensure the level of security offered will increase. CSPs are enhancing their capabilities for authentication, application security, data protection and data storage security.

2.2. *Industry perspectives*

Table 1 provides the notorious nine cloud security risks from Cloud Security Alliance (Cloud Security Alliance, 2013). Cloud security is a tractable problem and many of the concerns that arise with cloud security stem from either uncertainty or a lack of proper preparation. In fact, cloud computing can offer many advantages when it comes to security. Because security is such a 'hot button' issue, in many cases cloud providers overcompensate for security risks, sometimes dedicating entire security teams to monitor the system.

SaaS programs are based on multi-tenancy infrastructures. The biggest security risk with public SaaS providers is the associated risk of shared technology providers (Reval, 2012). Due to the shared nature of SaaS where one organization's applications may be sharing the same metal and databases as another firm, CISOs must recognize they do not have full control of these resources and consequently must question the inherent security of the cloud.

2.3. *Implementation concerns*

It is imperative that security needs are an early component of SaaS provider selection process (IBM, 2012). Too often when organizations adopt a SaaS program, they effectively undergo an entire requirements gathering, evaluation and selection process without including security.

The business then has chosen a SaaS provider and then expects security team to provide the necessary security either through contract negotiations and requirements or internal deployment. This ad hoc approach limits the ability to properly and effectively secure a SaaS program. Security needs to be an essential and major component of the original SaaS requirements and ongoing selection process (Intel, 2012).

3. Proposed FAGI methodology

3.1. *The importance of a holistic approach*

Evaluating vendors' capabilities is the crux of SaaS security (Samanage, 2013). SaaS providers are usually produce novels of documents covering anything and everything. IT security professionals must be able to sift through this chaos to find the things relevant to security concerns and requirements.

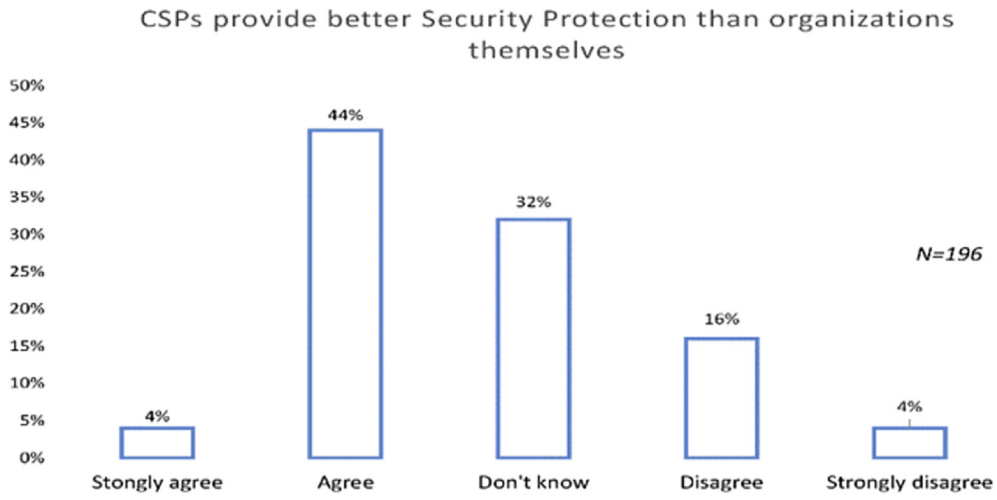

Fig. 4 – Security controls from CSP side. Note: color on the Web only.

There are several main reasons why we need a holistic approach to manage SaaS security risks.

1) With increased controls come increased responsibility. Organizations must readily adopt the auditor role of their providers to ensure security requirements are being met (EY, 2014). Consumers still need to take responsibility for their use of cloud computing services in order to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of the organization.
2) SaaS risks can be properly managed through a holistic approach to save time, money and effort. SaaS is not fundamentally insecure. It just needs to be managed and accessed in a secure and consistent way.
3) It will become more common practice for consumers to perform various in depth assessments of their providers in a variety of ways (Bell, 2013). Mature RFP and demos, questionnaires and response review, review of third party audit statements, on site audits and monitoring of cloud services are all becoming more and more effective and common.
4) There is a general shift within the SaaS market that is enabling consumers to have more power in contract negotiation and agreements. Although technical capabilities to secure a SaaS program are still limited, consumers are gaining negotiating power when determining required security controls.

3.2. *FAGI model*

Fig. 5 shows our proposed SaaS security framework, which aims to gauge the security assurance required by an organization and ultimately guide the organization in the selection of a trusted CSP. The level of security trustworthiness of a given CSP is dependent on four aspects: 1) the assurance that the CSP is able to deliver security functions that meet the organization's security obligations; 2) whether such security capabilities claimed can be verified through independent audits or assessments; 3) how transparent information relating the security of the cloud service is convey to the organization, in other words, the governability; 4) how easy it is for an organization to transfer from one CSP to another CSP for whatever reasons.

The FAGI model is rooted in security best practices and it is a superset of most adopted standards such as ISO27001/2(ISO/IEC, 2013), NIST SP800-53 (NIST SP800-53), CSA CCM (Cloud Security Alliance, CCM3.0, 2013a, b) and PCIDSS (PCISSC, 2013), as illustrated in Fig. 6. On the one hand, full security coverage is provided to organizations by FAGI model. Organizations are enabled to condense and streamline their

Table 1 – Notorious nine cloud security risks.

Cloud security risk	Description
Data breach	Sensitive or valuable data falling into the control of either malicious attackers or competitors.
Data loss	The possibility of seeing valuable data disappear without a trace.
Credential hijacking	Attacker gaining access to credentials for malicious intent.
Insecure interfaces and API's	Attackers can discover vulnerabilities within the scripts of interfaces and API's managing interfaces.
Denial of service	DOS attacks can make cloud programs unavailable, potentially bringing business to a standstill.
Malicious insiders	Angry or frustrated insiders of a CSP may have access to a network, system or data.
Cloud abuse	Attackers can use cloud networks increased computational powers for various malicious activities.
Insufficient due diligence	Lack of understanding of the cloud environment poses huge risks for all various cloud vulnerabilities.
Shared technology	One vulnerability or misconfiguration to compromise all data hosted on shared infrastructure.

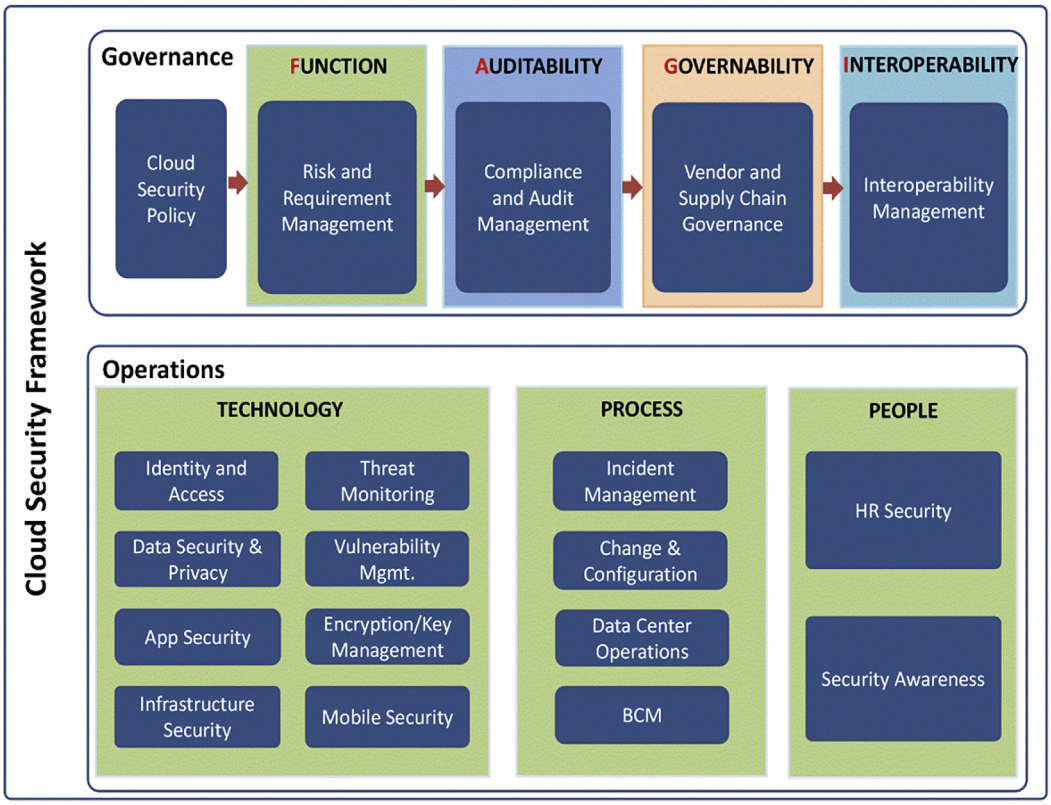

Fig. 5 – SaaS security framework. Note: color on the web only.

security management through implementing only one framework rather than having isolated and unconnected standards in place across the enterprise.

Table 2 shows the detailed mapping of FAGI components to controls required by CSA CCM, ISO/IEC 27001, NIST SP800-53 and PCIDSS.

A specific SaaS program has its own unique risk profile. Not all proposed FAGI components are necessarily needed by all organizations. A logic approach is needed to help an organization determine what security controls are required due to its specific SaaS risk posture, which is predominantly determined by the data sent to the cloud. Table 3 proposes main considerations for organizations to evaluate their SaaS risk profile which results in three possible postures: low, medium and high. Three classes of security controls (e.g. basic, strong and advanced) were recommended in alignment with the result of security risk posture analysis. Table 4 demonstrates recommended security controls based on risk posture analysis.

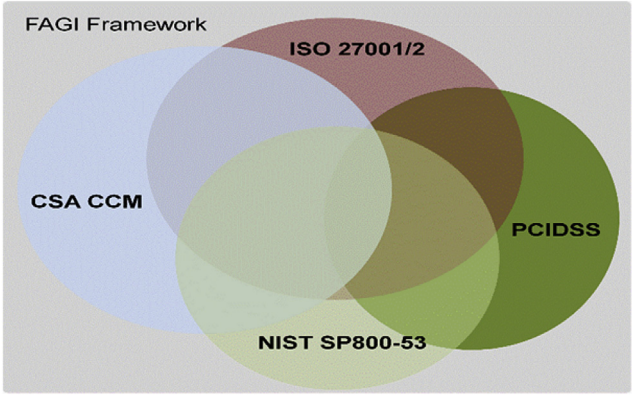

Fig. 6 – FAGI framework coverage. Note: color on the web only.

3.2.1. *Function*

One of the biggest challenges facing security professionals today is trying to concretely determine what security controls should be deployed and what provisions are covered in which SaaS provided documents and what are the specifics being stated.

The FAGI model has defined fourteen components for the security functions (shown as operations in Fig. 5) which reflect the full coverage of security requirements for almost all organizations. Table 5 demonstrates a further explanation of what should be included.

For each security control listed above, security requirements have been clearly defined in order to make FAGI framework actionable in the authors' research work. Due to length constraints, selected examples are listed in Table 6 below.

3.2.2. *Auditability*

One of the largest and most cited problems with SaaS vendors and their security offerings is a lack of transparency. Handing

Table 2 – Security components mapping.

FAGI model		CSA CCM	ISO/IEC 27001	NIST SP800-53	PCIDSS
Cloud security policy		GRM-06~09	Clause 4, 5, 7, A.5.1, A.8.2, A.10.1~2, A.14.1, A.15.2	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1~2, IA-1&5, IR-1, MA-1, MP-1,PE-1, PL-1&4, PM-1, PS-1&8	12.1~12.2
Function	Risk and requirement	GRM-01~05, 10~12	Clause 4.2~3,5,7.2~3, A.6.1~2, A.7.2, A.8.2, A.11.2, A.12.1	AC-4, AT-2~3, CA-1~3&5~7, CM-1~2&4, MP-8, PL-5, PM-1~11, RA-1~, SA-2&4, SI-12	1.1, 2.2, 12.1~12.2, 12.5~12.6
	Identity and access	IAM-01~13	Clause 4.3.3, A.11.1~2, A11.4~6, A12.4, A.15.1, A.15.3	AC-1~6, AU-1~6&9~14, CA-13, CM-1&5&7, IA-1~8, MA-3~5, PS-4~7, PM-10, RA-1&3, SA-7	3.5, 6.4, 7.1~2, 8.1~8.5, 9.1, 10.1, 10.5
	Data security & privacy	DSI-01~ 08	A.6.1, A.7.1~2, A.9.2, A.10.1, A.10.6~9, A.12.4~5, A.15.1	AC-2~6&11~16&21~22, AU-10&13, CA-2, CM-4, IA-8, MP-1&3&6, PE-1&16&19, PS-2, PM-5	1.2, 2.1, 3.1, 4.1~2, 6.4~5, 9.5~9.7, 9.10
	App security	AIS-01~ 04	A.6.2, A.10.8~9, A.12.2~6, A.15.1~2	AC-1&4, CA-1~2, CA-5~6, SC-1~21, SI-1~11	2.3, 3.4, 6.1, 8.3, 10.5
	Infrastructure security	IVS-01~ 20	A.7.1, A.9.2, A.10.1, A.10.3, A.10.6~10, A.11.1~6, A.12.3, A.13.1~2, A.15.1~2	AC-1&4&18, AU-1~14, CM-6, PE-4, SA-4, SC-2~3&7, SI-4	4.1, 6.4, 9.1, 10.1~7, 11.1, 11.4, 12.5, 12.9
	Encryption & key management	EKM-01~ 04	Clause 4.3.3 A.10.6~9, A.12.3, A.15.1	AC-18, IA-3, SA-1, SA-6, SC-7~28, SI-8	2.1, 3.4~3.8, 4.1~2
	Vulnerability management	TVM-01~03	A10.4, A.12.2, A.12.5~6	CM-3&4, CP-10, RA-5, SA-7, SC-5&8, SI-1~8	2.2, 5.1~2, 6.1~6.6, 11.2
	Mobile security	MOS-1~20	A.10.4, A.10.7, A.11	MP-2&~7, IA-1~3	1.4, 4.1
	Security threat monitoring	IVS-01	A.10.10, A11.2, A.11.5~6, A.13.1~2	AU-1~14, SI-4	10.1~10.7, 11.4, 12.5
	Security incident	SEF-01~05	A.6.1, A.8.2, A.13.1~2, A.15.1	AT-5, AU-6~7&9&11, IR-1~8, SI-4, SI-5	11.1, 12.5, 12.9
	Change & configuration	CCC-01~05	A.6.1, A.6.2, A.10.1~4, A.11.5~6, A.12.1~6, A.13.1, A.15.1~2	CA-1&6~7, CM-1~9, PL-1, PL-2&5, SA-1~13, SI-1~7	16.1~6.4,7.1, 8.5, 9.1~9.3, 10.5, 11.5, 12.3
	BCM	BCR-01~12	A.6.1, A.8.1~2, A.9.1~5, A.10.1, A10.7, A.14.1	CM-2~9, CP-1~10, MA-2~6, PE-1~18, RA-3, SA-1, SA-3~12	9.1~9.9, 12.1~12.4, 12.9
	Data center & operations	DCS-01~09	A.7.1, A.9.1~2, A.10.1, A.11.4	AC-17, CM-8, MA-1&2, IA-3~4, PE-1~18	9.1, 9.2, 9.8~9.10
	HR security	HRS-01~12	Clause 5.1, 5.2, A.6.1, A.7.1~2, A.8.1~3, A.9.1, A.10.7~8, A.11.3	AC-8&11&17~20, AT-2~5, MP-2~6, PL-4, PS-1~7, PM-10, SA-9, SI-5	8.5, 9.7~9.9, 11.1, 12.3~12.8
	Awareness	HRS-10	Clause 5.2.2 A.8.2.2	AT-1~4, PS1~7	12.6
Auditability	Compliance and audit management	AAC-01~ 03	Clause 4.2~3, 5.1~2, 6, 7.3 A.6.1, A.7.2, A.15.1, A.15.3	AC-1, AT-1, AU-1, CA-1~2&~7, CM-1, CP-1, IA-1&7, IR-1, MA-1, MP-1, PE-1, PL-1&6, PS-1, PM-1, RA-1~2, RA-5, SA-1&6, SC-1&13, SI-1&12	2.1, 3.1, 6.6, 11.2~11.3, 12.1
Governability	Vendor and supply chain governance	STA-01~09	A.6.2, A.10.2, A.10.6~8, A.11.4~6, A.12.3~5	CA-3, MP-5, PS-7, SA-6~7&9&12, SC-7&20~24	2.4, 12.8, PCI-DSS Appendix A
Interoperability	Interoperability management	IPY-01~05			

Table 3 – SaaS security risk posture considerations.

Component	Description
Company industry	Based on NAICS 2012. Profile the industry such as public administration, finance and insurance, or health care, etc.
Company type	Public company or private company.
Data & compliance	The criticality of the data stored/processed in the cloud. Profile compliance requirements such as PCIDSS, PIPEDA, HIPAA/HITECH, SOX, GLBA, FISMA, Bill198, and NERC etc.
Applications in the cloud	The types of applications operated by the organizations.
Security risk management	Organization's risk tolerance level; Risk visibility to the senior management and investors.
User community size	How many users will use cloud apps

off data doesn't hand off responsibility (Jan Stafford, 2013). Major problems arise from insufficient due diligence. You must become your vendor's auditor to get the security controls and confidence you need. With traditional IT environments you could directly secure and test it. With SaaS do the next best thing and verify your provider is doing it right.

Unfettered access to essential audit information is a key consideration of contracts and SLA terms with any cloud provider (Cloud-Council, 2012). Consumers should expect to see a report of the cloud provider's operations by independent auditors. As part of any terms, cloud providers should offer timely access to and self-management of audit event, log and report information relevant to a consumer's specific data or applications.

1) Use accreditation and certification to capture a snap shot of SaaS providers' security controls. Put on your auditor hat and ensure your SaaS vendor has an auditable SaaS offering or a fully assessed cloud by a third party certification or accreditation service.
   - A relatively simple and easy way to capture a snap shot the providers' security capabilities and maturity level is through accreditation and certification.
   - This consists of assessing any security certifications that your provider has. Various security certifications will provide you with a full overview of what they do in a quick period of time.
   - The most unequivocal assurances often provided in a cloud service agreement concern a provider's accreditations or certifications by one or more standard-developing organizations (SDOs) or their certified auditors.

The accreditations included in many agreements are intended to infer credibility without consumers needing to visit facilities and perform audits. Table 7 shows the most accepted third party certifications/assessments which organizations could leverage for assurance purpose.

2) If your provider is not certified by any industry security certifications, you must then assess their security controls

Table 4 – Recommended security controls based on risk posture analysis.

Risk posture	Low security risk posture	Medium security risk posture	High security risk posture
Proposed control class	Need basic (B) security controls 1) Note: Security controls in FAGI model are recommended and marked with B, S or A. However, organizations are encouraged to adjust the control classes according to their specific context. 2) Example: With respect to identity and access management, an organization with low security risk posture may only basic IAM solution. An organization with medium security risk posture may need conducting access activities monitoring. And organization with high security risk posture may also need to implement two-factor authentication.	Need basic and strong (S) security controls	Need basic, strong and advanced (A) security controls

Table 5 – List of security functions/domains.

Security domain	Security control	Class
Identity and access management	Access control policy	B
	Access control process and solutions	B
	Least privilege and segregation of duties	B
	ID credentials management	B
	Access activities monitoring and User access reviews	S
	Single sign-on and two-factor authentication	A
Data security & privacy	Data classification and data ownership	B
	Data inventory/flows and data jurisdiction/residence	A
	Data leakage protection	S
	Data preservation and redundancy	B
	Secure disposal	B
App security	Secure application development	B
	Production data protection	S
	Security testing	B
Infrastructure security	Configuration standard and OS hardening	B
	Computing virtualization security	B
	Network security	B
	Middleware and DB security	B
	Anti-malware	B
	Capacity and performance management	S
	Production/Non-production environments	S
	Mobile security	A
Encryption and key management	Encryption solutions	S
	Non-repudiation/digital signatures	A
	Key management	S
	Key escrow	A
Vulnerability mgmt.	Vulnerability management program	S
	Patch management	B
Security threat monitoring	Intrusion detection and prevention	B
	Log monitoring and analysis	S
Security incident management	Security incident management process	B
	Computer forensics	A
	Incident communication and reporting	S
	Security incident monitoring and metrics	S
Change & configuration	Changes from CSP	B
	Changes from consumer	B
BCM	Business continuity planning	S
	Business continuity testing	S
Data center physical and operations security	Controlled access points	B
	Asset management	S
	Data center utilities protection from environmental risks	A
HR security	CSP responsibilities	B
	Standard employment process	B
	Background screening	A
Awareness	Technology acceptable use	B
	Training/Awareness	S

yourself through various actionable and impactful tests as demonstrated in Table 8.

3.2.3. *Governance*

In the evolving world of cloud computing, there is a need for an effective management process for any problems that may arise. Today's reality is that cloud SLAs contain very limited information on consumer-provider management processes except possibly for large enterprises that are capable of negotiating unique terms (Linlin Wu, 2013). Implementing an effective management process is an important step to ensuring internal and external user satisfaction with cloud based services.

You need to develop strong vendor governance in order to realize a successful CSP relationship. In a client-service provider relationship, the client never loses accountability for business outcomes, despite the fact that an external organization is performing the work. A vendor governance framework enables the client to fulfill its accountability by exercising overall control and direction of the client-service provider relationship through a structure that links processes, resources, and business strategies and objectives.

Strong, viable SaaS providers should effectively create a high level of transparency across their internal security processes, internal monitoring activities, and notification capabilities (Jonas Repschlaeger, 2013). Evaluate SaaS providers based on their willingness to provide information and the

Table 6 – Security requirements examples.

Security domain	Security control	Security requirement
Identity and access management	User access reviews	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.
Data security & privacy	Data jurisdiction/ residence	1) Organizations with specific data location requirements must include contractual requirements identifying where data-at-rest (primary and replicated storage) shall be stored. For instance, the vendor shall identify all data centers that the data at rest or data backup will reside. All data centers will be guaranteed to reside within [defined boundary/country/ jurisdiction]. 2) Users should carefully consider as part of their data management strategy how the SLA will complement where their data will reside, where it is processed, and how this meets regulatory requirements. 3) Verification of new data location: Preferably the provider should be required to obtain the permission of the client to relocate the data before moving to a new location. Organizations should ensure that when a provider elects to provide its service from another location it will be required to notify its clients of the new location and provide a means for the client to independently verify where the data will be relocated.
Encryption and key management	Key management	1) Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). 2) Strong encryption (i.e. AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.
Security incident management	Security incident management process	Process shall be established to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.

level of granularity of that information. A provider resisting queries should be a red flag.

Many mature organizations have in place some sort of vendor sourcing process and governance. Adapt this framework from your own organization to create a security focused vendor selection process. This will ensure that you can easily integrate your security selection process into the larger SaaS vendor selection. Table 9 shows the major considerations organizations should pay attention to regarding to CSP governance.

3.2.4. *Interoperability*

One of the worst things that can happen with a SaaS program is trying to leave a vendor for another and realizing none of the pieces go together. You must evaluate SaaS providers on their ability to allow your data to be used in their software and then be transferred to another vendor or back internally if required. Interoperability is a key factor of cloud adoption.

Interoperability allows an organization to scale a service across multiple disparate providers on a global scale and have that system operate and appear as one system (The Open Group, 2014). Interoperability also allows the easy movement of data and applications from one platform to another, or from one service provider to another.

Interoperability is concerned with:

- Data, where applications and services share common data, or synchronization of some kind is required between data in-house and data in a cloud service.

Table 7 – Independent assessment report/certification examples.

Assessment type	Description	Class
SOC 2 Type 2 report	CSP should provide the latest evidence of SOC2 Type 2 report and update the status accordingly. Note: SOC1 (SSAE16), ISAE3402 and SOC3 reports are not valid for security purposes.	B
ISO/IEC 27001 certification	CSP should provide the latest evidence of ISO 27001 certification report and update the certification status annually.	S
CSA STAR certification	CSP should provide the latest evidence of CSA STAR (Security, Trust and Assurance Registry) 3rd-party assessment-based certification report update the status accordingly.	S
PCIDSS assessment report	CSP should provide the latest evidence of PCIDSS assessment report and update the certification status annually.	A
FedRAMP authorization	CSP should provide the latest evidence of RedRAMP authorization report update the status accordingly.	S

Table 8 – Self security test/assessment examples.

Assessment type	Description	Class
Access control test	Password complexity	B
	Secure log in process	B
	Segregation of duties	B
	Least of privileges	B
Vulnerability assessment	OWASP top 10 vulnerabilities	B
Penetration test	Evaluate the security controls from simulation of hackers	S
Data redundancy	The redundancy and recoverability of data	S
Security risk management process	The effectiveness of security risk assessment and treatment process	A
Security incident response process	The effectiveness of security incident response process	S
Data center physical access control	The effectiveness of physical access controls to CSP's data centers which host the client's systems and data.	A
DR plan	The capability to cover business system and process	S

- Process integration between applications/services, where one application or service invokes operations provided by another as part of some workflow.
- Management capabilities, which include the monitoring of cloud services and the control of cloud services. These include security capabilities such as Identity and Access Management.
- Business capabilities including usage reporting, invoicing and payments.

A lack of interoperability (and as a result portability) can lead to being locked to a particular cloud service provider. Put on your auditor hat to determine SaaS providers' level of interoperability provided. Table 10 demonstrates critical areas organizations should take into consideration when selecting a CSP partner.

4. Applying FAGI model to a real project

This section introduces a case study. In order to verify whether the FAGI framework works in the real world, we chose a Canadian district school board to conduct the pilot.

4.1. *Background*

This Canadian school board manages tens of thousands teachers and employees and hundreds of thousands students.

Table 9 – SaaS security governance considerations.

Item	Description	Class
Effective support process	A formal customized mutual-agreed service support process will be established between the consumer and CSP. The CSP will allocate dedicated team or resource in providing services to the consumer. Potential changes in the support processes or key personnel changes will be notified to the consumer.	B
	Monthly status meetings or other reporting/communication approaches preferred.	S
	A formal escalation procedure will be established.	B
	All security requirement pass along to the supply chain. Providers shall inspect, account for, and correct data quality errors and risks inherited from partners within their cloud supply-chain. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	
System/application availability	Monthly cumulative application availability should be reported (i.e.99.999%).	B
Service failure management/ Understand the disaster recovery plan	Service failure management outlines what happens when the expected delivery of a service does not occur.	B
Identity and access reporting	Provide auditing of all access to consumer data and applications.	A
Incident response and support	Process of reporting of security incidents and events with prioritization, notification and severity level assessment.	B
	Regular (i.e. monthly) reports includes the number of security incidents, the severity level, incidents closed, opening, etc.	S
	The support of computer forensics or e-Discovery	A
Change/enhancement/new service management	A formal procedure should be established on the planning and notification of SaaS application changes, enhancement or new services.	S
	Expiration of the business relationship and treatment of customer (tenant) data impacted	S
Data location notification	A formal procedure should be established on the management and notification data relocation.	A
Compliance support	The support of consumer's compliance activities should be clearly defined and documented such as vulnerability assessment, and penetration test, etc.	B

Table 10 – SaaS security interoperability considerations.

Item	Description	Class
1	The consumer should be able to terminate the agreement at any time, without penalty, provided sufficient notice is given to the provider.	B
2	There should be no additional cost associated with the exit process.	B
3	The CSP should be responsible for extracting consumer data from the IT environments, or at least aid the consumer in extracting their data by providing clear and concise documentation.	B
4	The provider shall use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications.	B
5	Transmission of data from the provider's cloud resources should leverage standard packaging and data transfer techniques.	B
6	All data and information belonging to the consumer should be maintained for a specific time period after transition and then be completely removed immediately after.Note: The typical time period is 1–3 months which gives the consumer sufficient time to find a new provider and to continue receiving service from the current provider in the interim.	S
7	The consumer should ensure that the CSP provides appropriate business continuity protection during the exit process.	S
8	At the completion of the exit process, the consumer should receive written confirmation from the provider that all of the consumer's data has been completely removed from the provider's IT environment. The written confirmation should also state that the provider agrees not to use the consumer's data for any reason in the future, including using the data for statistical purposes.	S

The school board has moved its email and calendar system, office system and IT service management system into the Cloud. It is planning to move more IT systems into the cloud. It has defined a standard of single sign-on infrastructure for cloud-based systems and applications.

4.2. *Major challenges*

This school board is very concerned about data privacy and compliance obligations including PCIDSS, and PIPEDA. An ad hoc approached was employed in a previous cloud related project. This school board experienced several serious security incidents due to insufficient security control designing and implementation, these arose, in part, due to a lack of capabilities by the CSP. The management team of this school board re-evaluated its approach and assumed a holistic framework to select and govern the trusted CSPs for the future cloud project engagements.

The school board defined these security challenges:

- No formal security framework and policies defined.
- Lack of mechanism to establish alignment and traceability of information security practices with school board's strategies and objectives and compliance requirements.
- Security is sometimes the last thing to be considered in the school board's information system design, and often gets relegated to the status of a few add-on fixes when all other design decisions have been frozen.
- Information security is viewed as solely a technical discipline.
- Lack of dedicated information security human resources.

4.3. *Design, selection and governance*

The school board adopted the FAGI model as a framework for their evaluation of the security requirements to mitigate the identified risks. Based on the FAGI model, the first task was to analyze the cloud security risk profile to determine which security functions should be employed. It was determined that their security risk posture was medium which in turn guided the selection of security functions (using the method explained in Section 3.2.1).

The process of selecting a CSP partner for this school board is to choose the most suitable CSP that is safe, auditable, governable and portable. Fig. 7 demonstrates the four imperative decisions to narrow down a qualified CSP.

- Decision 1: Select the safe cloud which meets all organizations' security functional requirements.
- Decision 2: Choose the auditable cloud through third party certifications/assessments or self tests.
- Decision 3: Pick out the governable cloud which provides the required transparency.
- Decision 4: Opt for the portable cloud which ensures the desired interoperability.

The defined risk profile and security requirements were used to define a request for proposals (RFP) document. The school board received RFPs from six CSPs in its initial RFP process. The six RFPs were then evaluated using the FAGI model and criteria mentioned above in a four step process. Table 11 shows the result that only one CSP met all the requirements. This selection process removes any possible bias regarding named brand CSPs to ensure that the vendor chosen meets the organization's needs.

In addition to the selection process, the school board determined that it required annual reports from the CSP for three separate audits; ISO/IEC 27001 Certification, CSA STAR Certification and PCIDSS Assessment Report were required from the CSP annually.

Furthermore, the board included the following core components into the agreement with CSP: termination condition and cost, data extraction and packaging standard, data migration and disposal. To complete their adoption of the CSP the board identified the need for enhanced governance, the

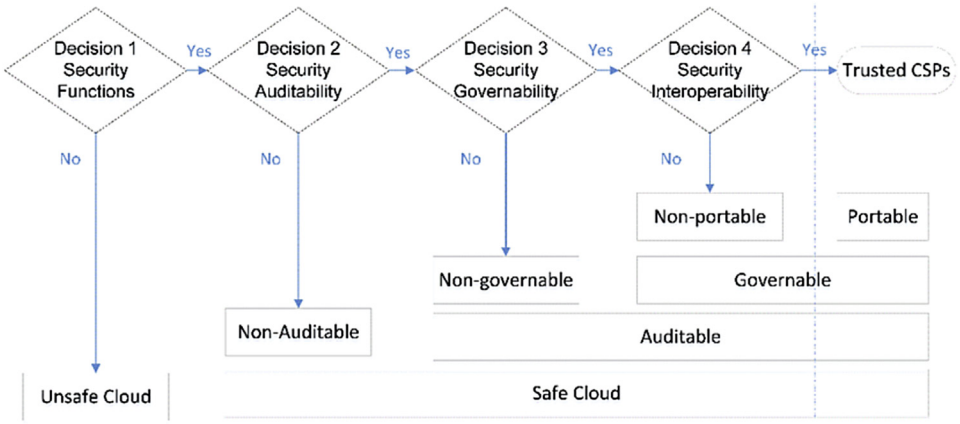

Fig. 7 – CSP selection process. Note: color on the web only.

board built a formal CSP governance procedure, a comprehensive security incident response process and a change management procedure.

4.4. *The result*

The CISO of the school board determined that use of the FAGI framework was a key to the achievement of the following goals:

- Built an unbiased, project-oriented and comprehensive trusted cloud security framework which supported the board engaging, evaluating and governing the trusted CSP.
- Security's needs were baked into the agreement with the CSP and project plan internally.
- Leveraged the security capabilities from SaaS vendors and avoided over-engineering or under-engineering security controls.
- Built and managed a win–win trust relationship between the board and the CSP.
- Minimized the security risks while leveraging the economic benefits of Cloud services.
- Gained confidence by ensuring organization's cloud environment is secured and protected from data leaks and breaches.

4.5. *Key insights from the case*

The top concern of data privacy can be mitigated using the FAGI framework. SaaS applications need to be managed and accessed in a secure and consistent way. Based on our initial findings FAGI provides a set of standard methods and steps to ease the issues that can prevent organizations from adopting cloud services. Here are the lessons learned from the case.

- It is imperative that security needs are an early component of SaaS provider selection. Security needs to be considered before even determining if you should adopt a public SaaS. You cannot glue on security after the fact.
- SaaS security is contingent upon proper and effective communication. You need to express your security requirements to two parties: First, your SaaS provider needs to know your requirements so these can be met and verified. Second, your internal SaaS project team needs to know the security requirements for project approval/sign off as well as appreciate the need for security.
- Although technical capabilities to secure a SaaS program are still limited, consumers are gaining negotiating power when determining required security controls. As more organizations adopt SaaS programs the light will be shed on these provisions. SaaS contract agreements will become more standardized and commoditized to empower the consumer.
- Understanding the interaction of cloud computing and the regulatory environment is a key component of any cloud strategy. If your data is regulated under any compliance standards, legislation or other legal control, you cannot skip some stipulation for convenience or some other benefits.
- Understanding the anatomy of a Cloud Service Agreement is the beginning of knowing what to do. Security obligations and privacy wording in SaaS artifacts can often be misleading or even damaging. One of the largest issues

Table 11 – CSP selection process and result.

	CSP1	CSP2	CSP3	CSP4	CSP5	CSP6
Function	YES	NO	YES	YES	NO	YES
Auditability	YES		YES	YES		NO
Governability	NO		YES	YES		
Interoperability			NO	YES		
Trusted CSP	NO	NO	NO	YES	NO	NO

when evaluating and comparing SaaS provider documents is there is no standard or common usage of the document artifacts among CSPs.

- Most providers address privacy only to the extent that they tell the consumer what data they will collect from the customer in order to provide the service. This is not what most consumers are concerned about when they think of "privacy in the cloud." They're not so much concerned about their own names and addresses, but rather about the private data they hold in the cloud about others.
- Do not forget to approach vendor governance with a relationship management mind set. Whereas the "science" of vendor governance is about having the appropriate structure, processes, and controls in place to achieve business outcomes, the "art" of relationship management is about facilitating alignment and maximizing the business value of the client-vendor relationship.

5. Conclusions

Organizations are moving toward the cloud. As a CISO or security professional you either have to adapt, or be left behind. The main challenges are to apply the same level of enterprise-class security controls internally to the cloud environment, obtain professional security audits of the cloud service, and to monitor usage for suspicious activity.

In this paper, we have presented the FAGI model, which tends to identify the security controls needed by an organization and guide the organization in the selection of a trusted service provider. Four components were structured to reflect the level of security trustworthiness of a given CSP: function, auditability, governability and interoperability. A logic approach was proposed to help an organization determine what security controls are needed in its specific SaaS context through analysis of organization's security risk posture. Three classes of security controls (e.g. basic, strong and advanced) were recommended in alignment with the result of security risk posture analysis.

A case study presented in this paper reveals that the structured and systematic approach proposed by FAGI can be an objective and effective process to save organizations' time, effort and grief regarding the selection of a qualified or trusted cloud provider. The next step is to incorporate maturity level assessment in FAGI model in order to provide organizations more flexibility and granularity to determine and select security controls that represent the best interest of their business strategies.

REFERENCES

Bell. Assessing the security of cloud service providers. 2013. Available at: http://www.bell.ca/enterprise/portlets/enterprise/documentform/core_content_downloads.jsp?FormId=CloudProviderSecurityAbilities&language=en [Last accessed: 08.16.14].

CCToffice. Security benefits of cloud computing. 2013. Available at: http://cctoffice.com/2013/03/security-benefits-of-cloud-computing [Last accessed: 07.14.14].

ChangeWave Research. Reasons why companies are not using the cloud. 2013. Available at: http://changewaveresearch.com/our-research/corporate [Last accessed 08.15.14].

Cloud Security Alliance. The notorious nine: cloud computing top threats in 2013. 2013. https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013 [Last accessed: 08.14.14].

Cloud Security Alliance. Cloud controls matrix v.3.0. 2013. https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3 [Last accessed: 08.16.14].

Cloud-Council. Security for cloud computing 10 steps to ensure success. Available at:. 2012. cloud security unfettered access to essential audit information www.cloud-council.org/Security_for_Cloud_Computing-Final_080912.pdf [Last accessed: 08.16.14].

CloudComputingAdmin. Standards and good cloud practice. 2014. Available at: http://www.cloudcomputingadmin.com/articles-tutorials/compliance-regulations/standards-and-good-cloud-practice.html [Last accessed: 08.14.14].

Dimension Data. Cloud security: developing a secure cloud approach. 2012. Available at: http://cloud.dimensiondata.com/am/en/about/resources/white-papers/cloud-security-developing-a-secure-cloud-approach [Last accessed: 08.14.14].

EY. Building trust in the cloud. 2014. Available at: http://www.ey.com/GL/en/Services/Advisory/Building-trust-in-the-cloud [Last accessed: 08.16.14].

HiMSS. Top 10 cloud security concerns introduction and overview. 2012. Available at: http://www.himss.org/ResourceLibrary/ResourceDetail.aspx?ItemNumber=10541 [Last accessed: 08.14.14].

IBM. Enterprise architecture in the age of cloud services enterprise architecture in the age of cloud services. 2012. Available at: http://www.ibm.com/developerworks/rational/library/enterprise-architecture-cloud [Last accessed: 07.10.14].

Intel. Intel's vision of the ongoing shift to cloud computing. 2012. Available at: www.intel.com/Assets/PDF/whitepaper/wp_cloud_vision_xeon.pdf [Last accessed: 07.10.14].

ISO/IEC. ISO/IEC 27001-information security management. 2013. Available at: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm [Last accessed: 08.16.14].

Jan Stafford. Enterprise cloud services: who's responsible?. 2013. Available at: http://searchaws.techtarget.com/opinion/Enterprise-cloud-services-Whos-responsible [Last accessed: 08.16.14].

Joyent. The compelling economics of cloud computing. 2012. Available at: http://www.joyent.com/content/06-developers/01-resources/16-the-economics-of-cloud-computing/compelling-economics-cloud-computing.pdf [Last accessed 08.15.14].

KPMG. The cloud changing the business ecosystem. 2011. Available at: http://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Pages/TheCloud-ChangingtheBusinessEcosystem.aspx [Last accessed 07.15.14].

PCISSC. PCI DSS v3.0. 2013. Available at: https://www.pcisecuritystandards.org/security_standards/pcidss_agreement.php?association=pcidss [Last accessed: 08.16.14].

Repschlaeger Jonas. Transparency in cloud business: cluster analysis of software as a service characteristics. 2013. Available at: http://link.springer.com/chapter/10.1007%2F978-3-642-38027-3_1 [Last accessed: 08.20.14].

Reval. SaaS technology: a medium for treasury change. 2012. Available at: www.reval.com/reval%20knowledge%20source/

RevalWhitePaper_12Mar12_SaaSTechnology.pdf [Last accessed: 07.10.14].
Samanage. Smart questions for your SaaS vendor. 2013. Available at: www.samanage.com/content/Smart-Questions-for-your-SaaS-vendor.pdf [Last accessed: 07.18.14].
The Open Group. Cloud computing portability and interoperability. 2014. Available at: http://www.opengroup.org/cloud/cloud/cloud_iop/cloud_port.htm [Last accessed: 08.25.14].
Wu Linlin. Automated SLA negotiation framework for cloud computing. 2013. Available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6546098&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6546098 [Last accessed: 08.16.14].

Changlong Tang holds a Master Degree (Software Engineering) and he is a PhD candidate at Beijing Jiaotong University. He had managed cyber security projects for over 80 clients across a wide spectrum of industries such as finance, government, healthcare, education, telecom, etc. His research interest includes: security strategy, security GRC, security assurance and metrics, and trusted could services. He holds several professional designations such as CISSP, CGEIT, TOGAF, CISA, CIPP/IT, CBCI, and PMP. He used to be an ISO27001/ISO20000/ISO9001 Leader Auditor and a PCIDSS QSA.

Jiqiang Liu is an Associate Professor of Beijing Jiaotong University. He was a visiting scholar at the University at Buffalo, USA. Jiqiang is the dean of Computer Engineering Department of Beijing Jiaotong University. His research interests lie in the areas of trusted computing, secure protocols, cryptography, privacy protection and model theory. He has published more than 50 papers.