Middle-East Journal of Scientific Research 23 (8): 1797-1803, 2015
ISSN 1990-9233
© IDOSI Publications, 2015
DOI: 10.5829/idosi.mejsr.2015.23.08.22482

Measuring the Security Compliance Using Cloud Control Matrix

T.N. Ravi and Sharmila Sankar

Department of Computer Science and Engineering,
B.S.Abdur Rahman University, Chennai, India

Abstract: Cloud computing has been identified as a promising and developing technology that provides development of large-scale, on demand, flexible computing infrastructures- hard ware and software. Globally number of Organizations today grapple with the expansion of distributed computing, increased online collaboration, explosive data growth and heterogeneous IT environments—all issues that make information security more critical, yet more complex than ever. Cloud computing has significant potential to improve security and resilience The Cloud provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures. There are different models / methods / standards are developed to provide guidance for implementing information security system for the clouds service providers. This research paper provides an overview for the implementation of cloud security alliance model Cloud control matrix (CCM). CCM provides the various controls needs to be implemented by the service provider to avoid / reduce / mitigate the risks related to the service provided. This helps in building the trust between the service provider and consumer on using the cloud services

Key words: Cloud security · Cloud customer · Cloud provider · Cloud security alliance · Cloud control matrix

INTRODUCTION

Cloud computing is an evolutionary outgrowth of previous computing approaches, which builds upon existing and new technologies. As per Winkler, "Securing the Cloud, Cloud Computer Security Techniques and Tactics"[1], Cloud computing represents a paradigm shift for delivering resources and services; this results in important benefits for both cloud providers and cloud consumers. From how we build IT systems and how we use them to how we organize and structure IT resources, cloud is refactoring the IT landscape. Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam [2] explains that the cloud computing change the Internet into a new computing platform, is a business model that achieves purchase on-demand and pay-per-use in network, has a broad development prospects. Unlimited storage for customers is one of the major benefits of cloud computing that reduce the concerns about the amount of remaining memory significantly. The advantage of the cloud is appealing: reduced costs, greater agility, flexibility, scalability, reduced cost of ownership and potentially greater security. At the same time, IT organizations recognize that the cloud introduces a number of issues related to security, data integrity, compliance, service level agreements and data architecture that must be addressed. Therefore, the adoption of cloud services is being tempered by a significant level of uncertainty. Efficient search is also an important concern in clouds. User privacy is also required so that the cloud or other users do not know the identity of the user. The validity of the user who stores the data is also verified [3]. Different cloud deployment models-public, private, or hybrid—have different security vulnerabilities and risks. Generally, risk increases from greater degrees of multitenancy among increasingly unknown participants Organizations use the Cloud in a variety of different service models (SaaS, PaaS and IaaS) and deployment models (Private, Public, Hybrid and Community). [1]

Cloud consumer / user choose the needed service based on various quality / process metrics for each services provide by the cloud provider. Numerous surveys indicate that the top concerns for moving to the cloud are: 1) security, 2) performance and 3) availability are the security concern about. Confidentiality, integrity and availability of information that is stored in the cloud.

Corresponding Author: T.N. Ravi, Department of Computer Science and Engineering,
B.S.Abdur Rahman University, Chennai, India.

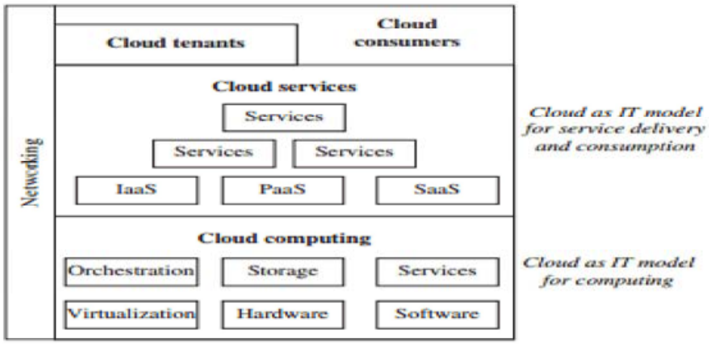

Fig. 1: Cloud computing

Confidentiality, Integrity and Availability: The overall objective for security is based on the triad of security: protecting the confidentiality, integrity and availability of information (referred to as CIA) [1].

- Confidentiality "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…. A loss of confidentiality is the unauthorized disclosure of information."
- Integrity "Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity…. A loss of integrity is the unauthorized modification or destruction of information."
- Availability "Ensuring timely and reliable access to and use of information…. A loss of availability is the disruption of access to or use of information or an information system."

Security of cloud services is a major concern to cloud consumers when selecting cloud providers. Sufficient security information should be provided so that consumer trust in cloud services can be built, but in practice, security information is critical and may not be publicized. As per Pumvarapruek, N during the service selection process, cloud consumers therefore have to study the available published information on the cloud providers' Web sites or the cloud provider's catalogue in order to assess how secure the services are [6]. However most of the cloud service providers are not providing the correct data related to the their security. It is generally recommended that information security controls be selected and implemented according and in proportion to the risks, typically by assessing the threats, vulnerabilities, impacts and probability of occurrence. There are many approaches are available for carrying out the risk assessment. For example ISO/IEC 27005-Information security risk management, IS /ISO 31000 "Risk management-principles and Guidelines" are most commonly used standards for the facilitating the risk management approach.

The cloud consumers are carrying out the risk assessment before the business migrates to cloud. R.Sabin Begum and Dr.G.Sugumar,in their paper "procuring cloud security using cloud control matrix", [4] discussed about the use of cloud control matrix, CCM V 1.4, developed by Cloud Security Alliance (CSA), for understanding the depth of information security system implemented by the cloud provider in their organization to protect the cloud consumer interests. In this paper the use of latest version of CCM V 3.0.1 is being discussed. CCM is freely downloadable from CSA website and will helpful for both the service provider and consumer to have an agreement on the need of the business. CCM provides a standard approach for the implementation of security controls by the service provider to identify and bridge the gap between needs of the customer and servicer provider.

The organization of this paper is as follows: Section 2 provides details about the security problems faced by cloud computing, Section 3 introduces the cloud control matrix, Section 4 details the domains of CCM and Section 5 details the approach for implementation of the controls of CCM. This paper end with concluding note and reference section.

Security Problem Faced by Cloud Security: Various surveys on Cloud computing adoption frequently identifies information security, loss of control, or similar issues as the top root causes that organizations hesitate to utilize cloud services. Enterprises are looking for assurances that they are not adding risk to the business by leveraging the cloud. Ironically, the virtualization and multi-tenancy that provide much of cloud's scalability, elasticity and potential cost benefits drive many of these security and privacy concerns. The protection afforded by traditional IT security perimeters is significantly challenged by the dynamic nature of large virtualized infrastructures that may spread over multiple geographic locations and involve assets beyond the immediate control of the organization [5-10].

As the data owner, the consumer maintains liability for protecting data to their end customer-internal or external, even if managed by a third party. Encryption is one of the solutions, but practical and business limitations exist for encrypting data in storage, data in transit and key management. Data in use remains vulnerable. Another important problem faced by the Cloud customer is the ownership of cloud service. Cloud consumer signs contract with a cloud service provider who intern get contract with the service provider such as Amazon cloud etc. to provide the service. In reality, the provider might have dependencies on other service providers (storage, network, application, processing, etc.) – none of which are necessarily obligated to the cloud consumer. These dependencies may change frequently without the consumer's knowledge, especially when cloud service providers are trying to meet elasticity and cost requirements. The consumer doesn't know where their data is and how or if it is being appropriately protected at any given moment. This daisy chain of trust may pose risks not addressed by contract and for which the consumer has no direct legal remedies.

In general the common security issues or questions that prospective cloud adopters face are

- Network Availability
- Privacy and Data.
- Control over Data.
- Cloud Provider Viability
- Security Incidents
- Disaster Recovery and Business Continuity
- Systems Vulnerabilities and Risk of Common Attacks

Regulatory or Legislative Compliance such as SOX, HIPPA, PCI etc.

In this paper Cloud Security Alliance's Cloud Control matrix is reviewed for its suitability to provide a solution to overcome or mitigate the above security issues.

Introduction to Cloud Control Matrix: The Cloud Security Alliance has created the Cloud Controls Matrix (CCM) which is a baseline set of security controls to help enterprises assess the risk associated with a cloud computing provider [7]. The Cloud Controls Matrix V 3.0.1 is aligned with CSA's guidance in 16 security domains, including application security, identity and access management, mobile security, encryption and key management and data center operations. CCM, which is part of the CSA Governance, Risk and Compliance (GRC) Stack, is mapped to multiple industry standards, regulations and frameworks that enterprises must follow, including ISO27001/27002, PCI, DSS, HIPAA and COBIT. [9].

CCM v3.0.1 is available as a free download to help organizations to evaluate cloud providers and guide security efforts. The matrix can also be used by cloud providers who wish to submit themselves to the CSA Security, Trust and Assurance Registry (STAR), a free publicly accessible registry that documents the security controls provided by cloud computing service providers. The Cloud Controls Matrix is designed to align well with the Consensus Assessments Initiative Questionnaire (CAIQ), a yes/no question set for identifying specific topics that a customer may want to discuss with potential cloud service providers. As a framework, the CSA CCM provides the organizations with the needed structure, details and clarity related to information security requirement tailored specifically towards cloud computing [4].

The CSA CCM Provides fundamental security principles to guide cloud vendors and to assist cloud customers in assessing the overall security risk of a cloud provider

- Strengthens information security control environments by delineating control guidance by service provider and consumer and by differentiating according to cloud model type and environment
- Provides a controls framework in 16 domains that are cross-walked to other industry-accepted security standards, regulations and controls frameworks to reduce audit complexity
- Seeks to normalize security expectations, cloud taxonomy and terminology and security measures implemented in the cloud [10].Organizations can use the CCM to develop a security compliance dash board and monitor the trend for compliance

CSA CCM V 3.0.1 includes;

- New or updated mappings to the following AICPA 2014 Trust Services Criteria
- Canada PIPEDA (Personal Information Protection Electronic Documents Act)
- COBIT 5.0
- COPPA (Children's Online Privacy Protection Act)
- CSA Enterprise Architecture

- ENISA (European Network Information and Security Agency) Information Assurance Framework
- European Union Data Protection Directive 95/36/EC
- FERPA (Family Education and Rights Privacy Act)
- HIPAA/HITECH act and the Omnibus Rule
- ISO/IEC 27001:2013
- ITAR (International Traffic in Arms Regulation)
- Mexico - Federal Law on Protection of Personal Data Held by Private Parties
- NIST SP800-53 Rev 3 Appendix J
- NZISM (New Zealand Information Security Manual)
- ODCA (Open Data Center Alliance) Usage Model PAAS Interoperability Rev. 2.0
- PCI DSS v3

Domains of Cloud Control Matrix: There are 16 domains identified in the CCM. They are

- Application and Interface Security
- Audit Assurance and Compliance
- Business Continuity Management and Op Resilience
- Change Control and Configuration Management
- Data Security and Information Lifecycle Management
- Datacenter Security
- Encryption and Key Management
- Governance and Risk Management
- Human Resources Security
- Identity and Access Management
- Infrastructure and Virtualization
- Interoperability and Portability
- Mobile Security
- Sec. Incident Management, E-Disc and Cloud Forensics
- Supply Chain Management, Transparency and Accountability
- Threat and Vulnerability Management

Approach to Implement Controls of Cloud Control Matrix: There are 133 controls in CCM V 3.0.1.Each domain has different number of controls. These controls are given with unique number and identification. The domain name and related number of controls are given in the Table 1

The CCM provides the details of the requirements for each of the control related to a specific domain area. Also these controls are linked with architectural relevance which helps the cloud consumer and provider to understand the relevance like physical server, network, computer, data, storage, application etc. Control requirement are given in the table 3.Sample control domain is given below in table 2 for the understanding from various domains.

The below table provides reference for each of the service model and supplier relationship with each control. This helps the service provider, consumer and vendor to understand their respective roles.

In addition to the above references, the CCM provides cross reference between each CCM control with other standards and models such as ISO 27001: 2013, COBIT 5, PCI 2.0, PCI 3.0,Jerico Forum, NIST, HIPPA. This helps the organizations to understand the effectiveness of implementation towards multiple standards and models.

Table 1: Control matrix

Domain name	# of controls
Application and Interface Security	4
Audit Assurance and Compliance	3
Business Continuity Management and Op Resilience	11
Change Control and Configuration Management	5
Data Security and Information Lifecycle Management	7
Datacenter Security	9
Encryption and Key Management	4
Governance and Risk Management	11
Human Resources Security	11
Identity and Access Management	13
Infrastructure and Virtualization	13
Interoperability and Portability	5
Mobile Security	20
Sec. Incident Management, E-Disc and Cloud Forensics	5
Supply Chain Management, Transparency and Accountability	9
Threat and Vulnerability Management	3

Table 2: Control Requirements

Control Domain	CCM V3.0 Control ID	Updated Control Specification
Application and Interface Security Application Security	AIS-01	Applications and interfaces (APIs) shall be designed, developed and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.
Business Continuity Management and Operational Resilience Business Continuity Testing	BCR-02	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.
Change Control and Configuration Management New Development / Acquisition	CCC-01	Policies and procedures shall be established and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.
Data Security and Information Lifecycle Management Classification	DSI-01	Data and objects containing data shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization, third-party obligation for retention and prevention of unauthorized disclosure or misuse.
Datacenter Security Asset Management	DCS-01	Assets must be classified in terms of business criticality in support of dynamic and distributed physical and virtual computing environments, service-level expectations and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly (or in real-time) and assigned ownership supported by defined roles and responsibilities, including those assets used, owned, or managed by customers (tenants).
Encryption and Key Management Entitlement	EKM-01	All entitlement decisions shall be derived from the identities of the entities involved. These shall be managed in a corporate identity management system. Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.
Governance and Risk Management Baseline Requirements	GRM-01	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and established and authorized based on business need.

Table 3: CCM V 3.0.1 –Architectural relevance

	Architectural Relevance						
CCM V3.0	--						Corp Gov
Control ID	Phys	Network	Compute	Storage	App	Data	Relevance
AIS-01		X	X	X	X	X	
BCR-02	X	X	X	X	X	X	X
CCC-01	X	X	X	X	X	X	X
DSI-01			X	X	X	X	X
DSC-01			X	X	X	X	X
EKM-01							
GRM-01	X	X	X	X	X	X	X

Table 4: Service provider and consumer relationship with controls

	Cloud Service Delivery Model Applicability			Supplier Relationship	
CCM V3.0.1					
Control ID	SaaS	PaaS	IaaS	Service Provider	Tenant/Consumer
AIS-01	X	X	X	X	X
BCR-02	X	X	X	X	X
CCC-01	X	X	X	X	
DSI-01	X	X	X	X	X
DSC-01					
EKM-01					
GRM-01	X	X	X	X	

Table 5: cross reference between each CCM control and other standards / models

	ISO/IEC 27001-2013	PCI DSS v2.0	HIPPA
AIS-01	A.11.5.6		
	A.11.6.1		
	A.12.2.1		
	A.12.2.2		
	A.12.2.3		
	A.12.2.4		
	A.12.5.2		
	A.12.5.4		
	A.12.5.5		
	A.12.6.1		
	A.15.2.1	6.5	45 CFR 164.312(e)(2)(i)
BCR-02	A.14.1.5	12.9.2	45 CFR 164.308 (a)(7)(ii)(D)
CCC-01	A.6.1.4		
	A.6.2.1		
	A.12.1.1		
	A.12.4.1		
	A.12.4.2		
	A.12.4.3		
	A.12.5.5		
	A.15.1.3		
	A.15.1.4	6.3.2	
DSI-01	A 7.2.1	9.7.1	
		9.10	
		12.3	
DSC-01			

CONCLUSION

From the above review of CCM it's understood that the Cloud security alliances Cloud control Matrix V 3.0.1 provides the needed support / understanding the relevance of security requirements for the Cloud consumer, provider and vendor and their roles and responsibility in implementing each control. This helps the cloud consumer to choose the service provider who meets their and end customer security requirements. However, each control may not be of importance to individual service provider and the consumer based on the service provided / consumed which is clearly identified in the table 4 To identify the specific control needs, organizations can introduce a weightage method to each control based on the risk assessment and measure the process compliance with a 1 to 5 scale and calculate the strength of compliance to the control.CCM helps in getting the security metrics for each service provider to compare and choose.

REFERENCES

1. VIC (JR) Winkler, Securing the Cloud, Cloud Computer Security Techniques and Tactics, Elsevier.
2. Moghaddam, Faraz Fatemi, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi and Shirin Dabbaghi Varnosfaderani, 2014. A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments, In proceeding of IEEE Region of Symposium, pp: 508-513.

3. Sushmita, Ruj, Milos Stojmenovic and Amiya Nayak, 2012. Privacy Preserving Access Control with Authentication for Securing Data in Clouds, In proceeding of IEEE International Symposium on Cluster, Cloud and Grid Computing, pp: 556-563.
4. Sabin Begum, R. and Dr. G. Sugumar, 2015. procuring cloud security using cloud control matrix, In proceeding of national conference on Information security and practices, pp: 9-11.
5. Balasubramian, R. and Dr. M. Aramuthan, 2012. Security problems and possible security approaches in cloud computing, International Journal of Scientific and Engineering Research, ISSN 2229-5518, 3(6).
6. Pumvarapruek, N., 2014. Classifying cloud provider security conformance to cloud controls matrix, Computer Science and Software Engineering (JCSSE), 2014 11th International Joint Conference on, pp: 268-273.
7. Cloud Security alliance, The Security guidance for critical areas of focus in cloud computing v3.0.
8. Cloud security alliance, Cloud Control Matrix https://cloudsecurityalliance.org/research/ccm.
9. Whitman Michael, E. and Herbert J. Mattord, Principles and Practices of Information security.
10. Cloud Security alliance, CCM v3.0.1 Information sheet,https://cloudsecurityalliance.org/research/ccm.