CLOUD COMPUTING AUDIT

Georgiana MATEESCU[1], Valentin SGÂRCIU[2]

This paper presents a personal approach of conducting the audit process in cloud architecture. Starting from the cloud computing benefits, we presented in Introduction section the main characteristics that a cloud provider should offer to his consumer in exchange for credibility and trust. In order to prove all these capabilities, a proper audit process must be implemented. Section 2 describes our original methodology of evaluating the safety level of a cloud service and the compliance level against the standards used as reference. Our personal contributions consisting in quantifying the safety level based on assumed risk level were validated by the implementation depicted in section three. This paper concludes with the benefits of our methodology.

Keywords: cloud computing governance, cloud audit, cloud strategy, cloud evaluation

1. Introduction

Cloud Computing is a very fashionable concept and in the same time, a controversial one. While a lot of people refer it as "a disruptive technology that has the potential to enhance collaboration, agility, scaling, and availability, and provides the opportunities for cost reduction through optimized and efficient computing" [1], there are a lot of opinions that think cloud computing is a trap for users to become cloud provider dependent [2].

The main attributes of cloud computing phenomenon are [3]:

- Shared resources – cloud computing is an architecture that allows multiple users to utilize the same resources from network level, host level to application level.
- Massive scalability – cloud computing has the ability to scale to thousands of systems.
- Elasticity – in cloud computing framework it is very easy to adapt the resources – hardware and software – to the user's necessity.
- Pay as you go – users pay only the resources they use for only the time they actually require them.

[1]PhD Student, Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania, e-mail: georgiana.mateescu@gmail.com

[2] Professor, Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania

- Self provisioning of resources – additional systems (processing capability, software, storage) and network resources are added if needed.

Cloud Computing represents a new architectural model that lead to new governance and management strategies based on the trust between consumers and providers. The trust it is defined by the level of security confidence a provider can offer to his clients, confidence that must ensure the following key factors [4]:

- Transparency in proving a high level of security measures implementation that assures the proper use of confidential data during their entire lifecycle: create, share, use, archive, destroy stages.
- Privacy – the cloud services must prevent, detect and react to security breaches and malicious attacks in a timely and effective manner.
- Compliance – the cloud provider must prove compliance with the security standards and regulations. One of the most important aspects regarding this topic is to ensure that the cloud consumer is able to retrieve his data from the cloud whenever is required.
- Localization of data – the physical location of the data storage can be the subject of particular regulation is some geographic area, therefore the consumer must ensure proper cloud provider selection if his activity is in scope for such standards.

In order to prove that the cloud service is compliant with technology and security requirements, a proper audit process must be conduct. In this paper, we present our personal approach in defining an effective audit methodology, able to quantify the cloud service safety and compliance based on the key drivers from the main areas concerning the IT infrastructure: governance, management, operations.
Starting from the COBIT [5] framework we have created an original approach to evaluate the safety of a cloud service in order to emphasize the main areas where enhancements are required. The next section describes the cloud audit methodology together with the evaluation algorithm. The third section presents the practical implementation for methodology validation. This paper concludes with the main advantages and benefits of the presented approach.

2. Cloud Audit Process

The Cloud Audit is a relatively young domain that is being enhanced by the cloud practices and standardization communities in order to address all particular issues of the kind of architectural model. The current practice, started from the IT traditional security and control measures are based on these, the audit process is being continuously customized on the cloud specific particularities.
In order to create this approach, we started from the existing principles, best practices and recommendations regarding audit process, we mapped the traditional architectures with the cloud models in order to define the main

verticals for the cloud audit specific characters and for all these verticals we classified them into domains. The categorization was performed according to the security reference model defined in [7]. For all the verticals we defined controls able to measure them.
After defining the audit context and aspects to evaluate, we built our evaluation methodology based on COBIT [5] model that offers a framework used to assess the governance and the management of IT. The framework was initially designed on traditional architecture, but it can be adapted to cloud architectures also.
The capability model leveraged by our methodology is depicted in the picture below:

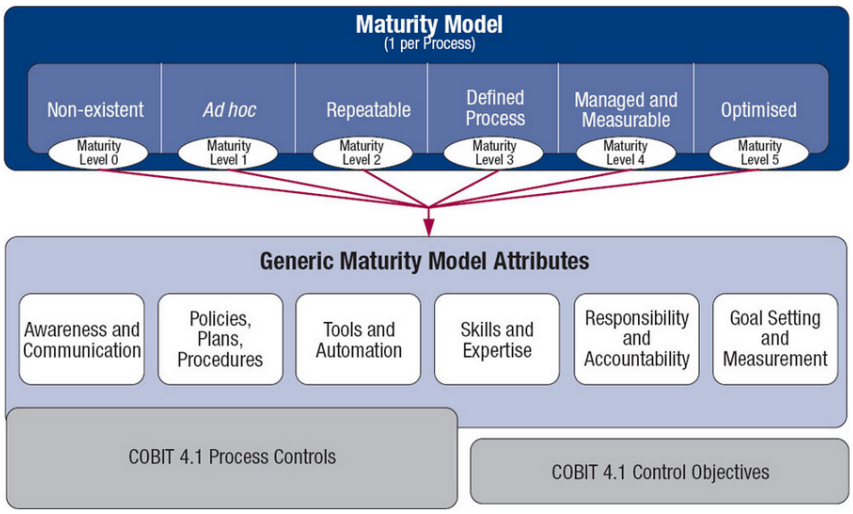

Fig 1: COBIT capability model [5]

In order to conduct the audit process, we structured the existing IT key principles [6], practices, mechanisms, procedures and controls in 14 domains, according to [7]. The audit process addresses one cloud application that is evaluated from one or multiple security domains perspective [8] [9], by analyzing the implementation level of each control defined in the audit questionnaire for that domain.
The audit report consists in two main drivers:

- The safety level – this represents the level of security controls implementations as compared to the assumed risk defined for the application that is been evaluated.
- The compliance level – this represents the percentage of the security coverage in the analyzed domains as they are defined by CSA in [7].

In order to compute the Safety Level, the approach defines the application risk as the uncertainty rate reported to the cloud vulnerabilities from the analyzed security domain, materialized in the implementation level of each control:

$$AR_i = c_{NSA} + \sum_{k=1}^{n} (5 - s_k) \cdot c_A \quad (1)$$

Where:

- AR_i is the application risk for the evaluated domain *i*
- c_{NSA} is the correction risk constant computed based on the existing cloud community experience. Its value is 0.01 and it is introduces for practical reasons because there is no domain with zero risk.
- s_k is the score of the implementation level for control *k* from the domain *i*
- c_A is the correction constant applied to the risk defined for the control.

This constant depends on the industry the target belongs to, and on the sensitivity level of the cloud service.

- *n* is the number controls being evaluated in the audit process

For each cloud application, there is an assumed level of risk ranked from 1 to 3, defined by the IT strategy and management responsible team. Based on the assumed level of risk, the assumed risk is computed using the following expression:

$$AR'_i = RL \cdot n \cdot c_A \quad (2)$$

Where:

- AR'_i is the assumed risk for the evaluated domain *i*
- *RL* is the risk level defined by the management responsible team
- c_A is the correction constant applied to the risk defined for the control.

This constant depends on the industry the target belongs to, and on the sensitivity level of the cloud service.

- *n* is the number controls being evaluated in the audit process

Based on these two measures, the safety level is computed as:

$$SL_i = \frac{5n(1 - c_A) - AR_i / AR'_i}{5n} \cdot 100 \quad (3)$$

Where:

- SL_i is the safety level for the evaluated domain *i*
- c_A is the correction constant applied to the risk defined for the control. This constant depends on the industry the target belongs to, and on the sensitivity level of the cloud service.
- AR'_i is the assumed risk for the evaluated domain *i*
- AR_i is the application risk for the evaluated domain *i*

- n is the number controls being evaluated in the audit process

If the audit process is conducted for multiple domains, the safety level is the arithmetic mean of the safety levels of the individual domains:

$$SL = \frac{\sum_{i=1}^{n} SL_i}{n} \tag{4}$$

Where:

- SL is the safety level of the audit process
- SL_i is the safety level for the evaluated domain *i*
- n is the number of domains in scope for the audit process.

Based on the safety level and on the assumed risk level, the Compliance Level is computed using the following expression:

$$CL_i = \frac{1+(-1)^c}{2}(SL_{\min} + \frac{SL_i - SL_{\min}}{SL_{\min}}) \tag{5}$$

Where:

- CL_i is the compliance level for the evaluated domain *i*
- SL_i is the safety level for the evaluated domain *i*
- n is the number of domains in scope for the audit process
- c is the compliance factor that ensure that the compliance level is zero if the minimum safety level is not reached. This factor is computed using the following expression:

$$c = \begin{cases} 1, SL_i < SL_{\min} \\ 2, SL_i > SL_{\min} \end{cases} \tag{5}$$

- $SL_{\min}$ is the minimum safety level that must be obtained by a domain in order to be compliant and it is computed based on the assumed level of risk:

$$SL_{\min} = 1 - RL \cdot c_c \tag{6}$$

Where:

- $SL_{\min}$ is the minimum safety level
- RL is the assumed risk level for the application
- c_c is the compliance constant and its value is 0.25

The compliance level is the measure of the implemented level of security and governance measures, as compared to the best practices recommended by the standards used as references when we defined the audit framework.

Therefore the two levels computed by our approach offer a realistic view of the contracted cloud service by analyzing the entire integration context. Our approach analyzes both cloud provider and consumer controls in order to evaluate the level of performance, governance, risk, management and operation of the IT domain.

3. Implementation the audit process

In order to validate the proposed methodology we used the following architecture:

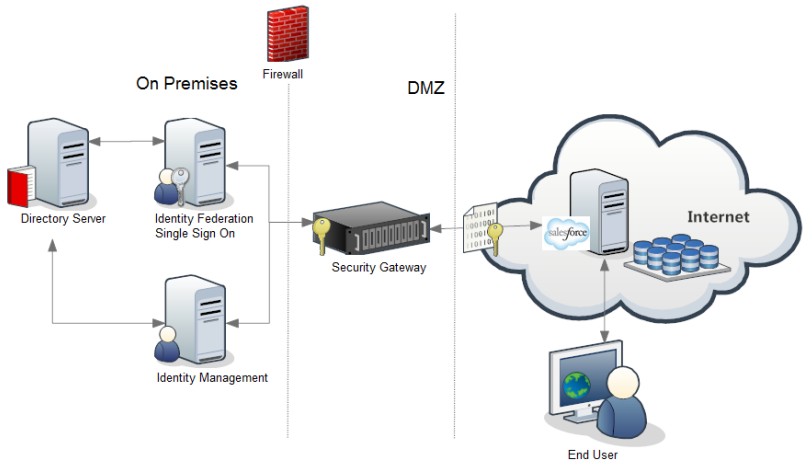

Fig 2: Implementation Architecture

The IT environment components are:

- The Identity Management System in charge with the management of the enterprise users and accounts in target systems. This system retrieves identities attributes from Directory Server system and, based on defined business rules, provisions the cloud service through APIs calls. The communication between Identity Management and salesforce.com is authenticated and the information flow is encrypted by the Security Gateway. Identity Management is the system that manages the users and the roles within salesforce.com..
- The Directory Server system is the authoritative source of identities attributes in the company and provides all employees details to Identity Management system.
- Identity Federation and Single Sign On system is the system in charge with the authentication process within the company. The repository for the identity federation is Directory Server
- Security Gateway is the system in charge with the encryption of data in motion involved in the integration with salesforce.
- Salesforce.com is the cloud service that is been audit and has the following characteristics depicted by the Table 1 below.

Table 1

The audited application characteristics

No	Characteristic	Value
1	Application Name	Salesforce.com
2	Sensitive Application	No
3	Nivel de Risc Asumat	2
4	Implementation Program	Salesforce
5	Cloud Service Type	SaaS
6	Cloud Model	Cloud Public

During the audit process we addressed 11 domains out of 14 because these were the most relevant ones:

- Governance and Enterprise Risk Management [14]
- Traditional Security, Business Continuity and Disaster Recovery [13]
- Compliance and Audit [18]
- Portability and Interoperability [17]
- Incident Response, Notification and Remediation [13]
- Application Security [11]
- Encryption and Key Management [18]
- Identity and Access Management[15]
- Virtualization [16]
- Data Center Operations [19]
- Information Management and Data Security [12]

The table below depicts the audit results:

Table 2

Audit Results

Domain	No of Controls	App Risk	Assumed Risk	Safety Level
Governance and Enterprise Risk Management	41	0.65	0.82	0.982266508
Traditional Security, Business Continuity and Disaster Recovery	17	0.18	0.34	0.977543253
Compliance and Audit	40	0.41	0.8	0.984875
Portability and Interoperability	8	0.14	0.16	0.94625
Incident Response, Notification and Remediation	17	0.35	0.34	0.965778547

Domain	No of Controls	App Risk	Assumed Risk	Safety Level
Application Security	12	0.23	0.22	0.951983471
Encryption and Key Management	33	0.67	0.66	0.977695133
Identity and Access Management	62	0.7	1.22	0.986237571
Virtualization	10	0.11	0.2	0.968
Data Center Operations	17	0.13	0.34	0.98100346
Information Management and Data Security	5	0.01	0.1	0.982
Total Number of Controls	262	Safety Level		0.97305754

The following picture depicts the ratio between the Application Risk computed during the audit process and the Assumed risk for the analyzed domains:

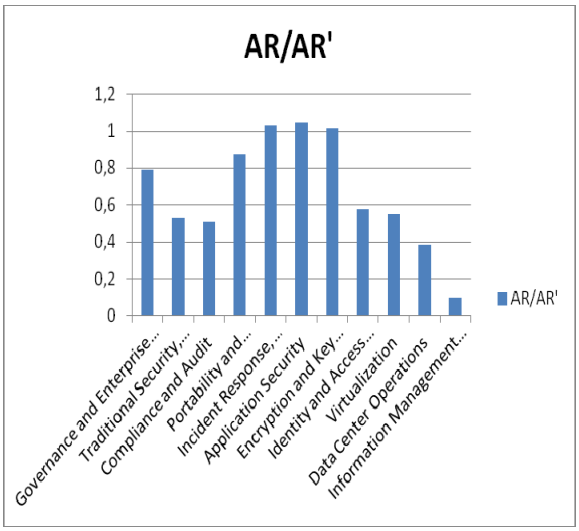

Fig 3 Ration between Application Risk and Assumed Risk

The picture shows that the domains where the audited application risk exceeded than the assumed risk are:

- Incident Response, Notification and Remediation
- Application Security
- Encryption and Key Management

For these domains, the company will have to enhace the existing controls in order to ensure that the risk is addressed properly and the business requirements regading availability and auditability are met.

The picture below depicts the comparison between the safety level computed during the audit process for all in scope domains:

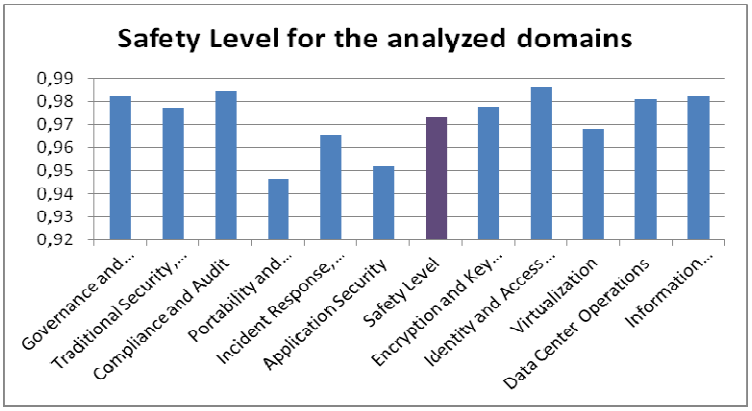

Fig 4: Safety Levels

The level of safety of the audited application is $SL = 97\%$. Considering that the assumed level of risk is $RL = 2$ and that the application is not considered sensitive, the minimum safety level that must be met in order for one domain to be compliant is:

$$SL_{\min} = 1 - RL \cdot c_c = 95\% \tag{7}$$

Based on the minimum safety level, the conformity level is computed for each in scope domain and the results are presented in the picture below:

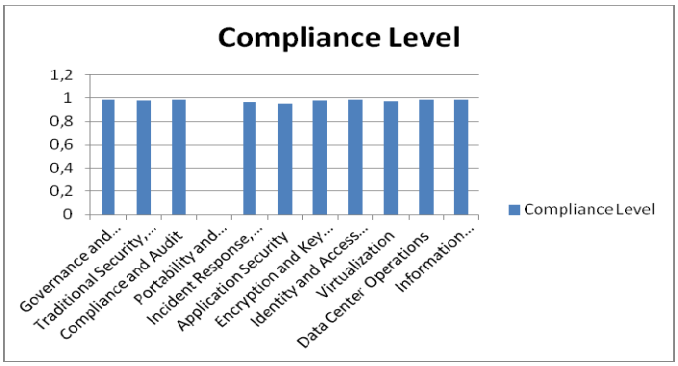

Fig 5: Conformity Levels for the analyzed domains

We can conclude that 10 out of 11 analyzed domains are compliant with the best practices recommended by the standards used as references in the audit

approach. The only domain that was not compliant is Portability and Interoperability which safety level is 94.62%. This means that the efforts for performing the enhancement required for compliance are not significant as the difference until the minimum safety level in very small.
The mean compliance level for the 10 compliant domains is:

$$CL = \frac{\sum_{i=1}^{10} CL_i}{10} \cdot 100 = 97.7\% \quad (8)$$

We can conclude that the audited service cloud is a safe service, with the safety level of 97% that proves the high performance security and control mechanisms in place in order to ensure transparency, privacy, availability and required performance.
In the architecture we audit, the salesforce.com was compliant in 10 domains out of 11, fact that leads to a 90.9% percentage of compliance. As already mentioned, the difference between the safety level on the non-compliant domain and the minimum safety level required for compliance is small, therefore the overall evaluation of salesforce.com is classifying this service as a safe, controllable and high performance cloud service.

By implementing this use case we proved the practical applicability of our approach in evaluating the cloud service form the following perspectives:

- Security controls in place in the architecture on both costumer and provider side
- Governance and risk management measures
- Operability processes and procedures

6. Conclusions

Nowadays the information security and profitability are maybe the most important two aspects within an organization. They are interconnected and have a direct impact one on each other and because of that the main challenge today is to find the best balance between the cost spent on the security aspects and their profitability. In order to ensure the maximized business value added by implementing IT programs, the companies must build a strong audit process able to quantify the safety of the IT solution implemented, the profitability rate and the IT strategy maturity.
By combining technical aspects [10] dived into main security drivers with governance and operations related factors, we managed to offer a full evaluation analysis of cloud system that quantifies the overall safety of the cloud safety from both technological and operational perspective. In this way, the audit process can be a key decision support for the IT strategy roadmap.

Our approach offers the following benefits and innovations:

- Quantifies the safety score based on security measures and controls using an original methodology based on mature and reliable framework.
- Quantifies the level of compliance with the standards used as reference in defining the audit framework. The approach relies of the safety score and it is built by adapting the traditional methodology to cloud architectures.
- Offers an efficient methodology for complex analysis that shows strengths and weaknesses of the company
- Offers decision support for future cloud adoption by evaluating the rate of company maturity and adaptability to change by assessing the entire stack of mechanisms, controls, process and procedures defined within the company in order to obtain an efficient governance and management process.
- By using as a reference model an international standard, we ensure that the principals, best practices and mature recommendations are part of the audit process. Also, by leveraging an existing framework for initial assessment of the implementation level, we obtain all the benefits of a framework that proved its value during the experience.

We can conclude that our approach helps the company gain visibility on their own IT environment by evaluating the governance, management and operations maturity levels using a holistic approach.

REFERENCES

[1] *Cloud Security Alliance*, "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0" 2011

[2] *Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia*, "Above the Clouds: A Berkeley View of Cloud Computing" Electrical Engineering and Computer Sciences University of California at Berkeley – Technical Report February 10, 2009

[3] *Tim Mather, Subra Kumaraswany, Shahed Latif*, „Cloud Security and Privacy. An Enterprise Perspective on Risk and Compliance", O'Reilly United States of America, first version 2009

[4] *Robert R. Moeller*, Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL, 2013 John Winley & Sons ISBN:9781118138618

[5] *ISACA*, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, 2012, ISACA ISBN:9781604202373

[6] *ISACA*, IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, 2011, ISACA ISBN:9781604201826

[7] *Cloud Security Alliance*, Security Guidance for critical areas of focus in cloud computing v3.0, 2011 https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[8] *Robert R. Moeller*, Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL, 2013 John Winley & Sons ISBN:9781118138618

[9] *Jared Carstensen, Bernard Golden, JP Morgenthal*, Cloud Computing: Assessing the Risks, 2012, IT Governance ISBN:9781849283595
[10] *Chris Davis, Mike Schiller, Kevin Wheeler*, IT Auditing: Using Controls to Protect Information Assets, Second Edition, 2011 McGraw-Hill/Osborne ISBN:9780071742382
[11] *Lee Newcombe*, Securing Cloud Services: A Pragmatic Approach to Security Architecture in the Cloud, 2012, IT Governance ISBN:9781849283960
[12] *Jennifer L. Bayuk*,Cyber Security Policy Guidebook, 2012, John Wiley & Sons ISBN:9781118027806
[13] *Kurt J. Engemann and Douglas M. Henderson*, Business Continuity and Risk Management: Essentials of Organizational Resilience, 2012, Rothstein Associates ISBN:9781931332545
[14] *Robert R. Moeller*, COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance, Second Edition, 2011, John Wiley & Sons ISBN:9780470912881
[15] *Matthew Metheny*, Federal Cloud Computing: The Definitive Guide for Cloud Service Providers, 2013, Syngress Publishing ISBN:9781597497374
[16] *Diane Barrett and Greg Kipper*, Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments, 2010 Syngress Publishing ISBN:9781597495578
[17] *Nick Antonopoulos, Lee Gillam*, Cloud Computing: Principles, Systems and Applications, 2010, Springer ISBN:9781849962407
[18] *Ben Halpert*, Auditing Cloud Computing: A Security and Privacy Guide, 2011, John Wiley & Sons ISBN:9780470874745
[19] *Brian J.S. Chee, Curtis Franklin*, Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center, 2010, Auerbach Publications ISBN:978143980612