Chapter 69
Compliance in the Cloud

Lucia Bonelli
Engineering Ingegneria Informatica, Italy

Angelo Immediata
Engineering Ingegneria Informatica, Italy

Luisa Giudicianni
Engineering Ingegneria Informatica, Italy

Antonio Luzzi
Engineering Ingegneria Informatica, Italy

ABSTRACT

Despite the huge economic, handling, and computational benefits of the cloud technology, the multitenant and geographically distributed nature of clouds hides a large crowd of security and regulatory issues to be addressed. The main reason for these problems is the unavoidable loss of physical control that costumers are forced to accept when opting for the cloud model. This aspect, united with the lack of knowledge (i.e. transparency) of the vendor's infrastructure implementation, represents a nasty question when costumers are asked to respond to audit findings, produce support for forensic investigations, and, more generically, to ensure compliance with information security standards and regulations. Yet, support for security standards compliance is a need for cloud providers to overcome customers hesitancy and meet their expectations. In this context, tracking, auditing, and reporting practices, while transcending the compliance regimes, represent the primary vehicle of assurance for security managers and auditors on the achievement of security and regulatory compliance objectives. The aim of this chapter is to provide a roundup of crucial requirements resulting from common security certification standards and regulation. Then, the chapter reports an overview of approaches and methodologies for addressing compliance coming from the most relevant initiatives on cloud security and a survey of what storage cloud vendors declare to do in terms of compliance. Finally, the SIEM-based approach as a supporting technology for the achievement of security compliance objectives is described and, the architecture of the security compliance component of the VISION Cloud architecture is presented.

INTRODUCTION

Although the distributed computing models and virtualization technologies have introduced substantial benefits, the facts that both physical and software resources can be geographically distributed and shared by different users and the customer has not control over the physical security of the infrastructure that host their business services, have heightened the common security and regulatory issues of traditional IT infrastructure.

DOI: 10.4018/978-1-4666-6539-2.ch069

As a result, it is fundamental for a cloud provider to guarantee and demonstrate that the security level of its infrastructure is at least the same of the customer's one.

According to this, most important initiatives on security compliance, including CSA (Cloud Securtiy Alliance) and ENISA – European Network and Information Security Agency, emphasizes the importance to certify the cloud offering to the common security standards such as ISO27001 and PCI-DSS and audit framework such as SAS-70 II, in order to cushion cloud computing security issues.

Providing evidence of adherence to these standards is binding for cloud providers that are supposed to host critical applications or sensitive data. For example: getting PCI DSS certification is mandatory in the context of for credit card management system, while HIPAA prescribes a rigorous security checklist in order to preserve the integrity and confidentiality of personal health records.

Among the key requirements derived from these standards, the aspect of auditing and its impact to the cloud computing is sticking out more and more. It implies the need for cloud provider to put in place logging management and reporting mechanisms in order to gather information about the behavior of the hardware, software and network infrastructure used to run specific tenant applications, and process them to elaborate security and compliance reports that are needed for audit purposes. In synthesis, logging and reporting practices are essential for auditor and management to control on the compliance objectives achievement.

In this chapter, the privacy compliance and the storage infrastructure compliance regulations and standards and their applicability to storage clouds, as well as the derived key requirements, are firstly discussed. Then an overview of the most accredited works on security compliance best practices, recommendations and guidelines in the cloud is provided, along with a survey of how the most common cloud providers approach the problem of compliance.

Finally, the chapter presents the architecture of the VISION Cloud compliance component is presented. It is a SIEM (System Information and Event Management) based, scalable and flexible system that can be deployed in a variety of distributed and virtualized infrastructure and which provides the following capabilities: collection in a secure way of audit records from different sources (and in different format) of the distributed infrastructure, normalization records in a standard an common format independent from the source, application of security polices over the normalized messages and (in case of events that may require corrective actions or other types of responses) generation of alert, summary of data in reports in conformity with ISO 27001.

THE PROBLEM OF BEING COMPLIANT

Security responsibilities of both the provider and the consumer differ between cloud service models. Security controls, at a glance, can be divided into three macro-areas which directly derive from the corresponding cloud service models defined above. The first ones are Infrastructure-Level (IL) security controls. Controls performed at this level can refer up to the physical, environmental and virtualization layers. The second ones are Platform-Level (PL) security controls. Controls performed at this level can refer up to the operating system and running environment layer. The last ones are Software-Level (SL) security controls. Controls performed at this level can refer up to the application layer.

As an example, Amazon EC2 IaaS offering can provide only IL security controls while PL and SL are fully missed. The reason for that is the lack of knowledge about the applications that will run upon the virtualized infrastructure and, more important, the type of managed data and data pro-