Chapter 6
Compliance and Regulatory Standards for Cloud Computing

Jitendra Singh
JIT University, India

Vikas Kumar
Asia-Pacific Institute of Management, India

ABSTRACT
Cloud computing is expanding in reach, with its utility-based features and enhanced agility. Still, there is a big concern about the privacy and security of the data. Because of these concerns, third-party cloud users are employing the cloud only for less sensitive data, and the advantage of cloud computing is not fully harnessed. In order to ensure the privacy and security of data, proper compliance and regulatory standards become very important for the cloud domain. Although a number of such standards exist for the traditional computing, they must be modified for their wider adoption to the cloud platforms. This chapter considers the worldwide available standards in the technical and non-technical categories for wider coverage of the cloud platforms. In the technical category, security standards presently followed by cloud computing have been discussed, while in the non-technical category, privacy and accounting standards like HIPPA, SAS 70, GAPP, etc. have been considered.

INTRODUCTION
Cloud computing is the imagination of Leonard Kleinrock (2005) one of the scientist at Advance Research Project Agency. In 1969 he said: “As of now, computer networks are still in their infancy, but as they grow up and become sophisticated, we will probably see the spread of ‘computer utilities’ which, like present electric and telephone utilities, will service individual homes and offices across the country”. This concept remained in dormant stage before 90s, and re-emerged in mid-90s with the effort of companies like HP, IBM, and Amazon, etc. (Armbrust, Armando, Rean, et al., 2009). On demand self service, Elasticity, Measured service, Broad network access and Resource Pooling are the five tenets of the cloud, which are widely accepted including by the cloud security

DOI: 10.4018/978-1-4666-4209-6.ch006
alliance (Cloud Security Alliance, 2009) and in NIST (Mell and Grance, 2009). It is envisaged that services and applications will migrate to cloud from where it will be accessed by users using different type of devices for, e.g. terminal, PDA, Smartphones, etc. A number of vendors exist to provide cloud services and to take the lead in this new paradigm. These service providers are using their own proprietary APIs to enable the smooth communication among users and other cloud providers. However, because of proprietary APIs there is always a concern among the users that they may stick in lock-in at a later stage. As users can access cloud services from disperse locations of the globe, there is a big concern among the users about the security. Despite the trumpet business and technical advantages, numbers of potential cloud users are yet to join, and those who have joined are putting less sensitive data (Chow, 2009).

Control in the cloud is one of the major concerns among various users in adopting the cloud because it requires implementation of regulatory compliance and to ensure privacy of the data maintained. “As enterprises start to run their entire networks on the cloud, existing certifications [such as Gramm-Leach-Bliley, etc.] start to break down” (Lamont, 2009). The certifications assume that the enterprise controls everything, and it’s all located within their office building, however the situation is not true with the cloud platforms. Corporate and offshore partnership requires similar enforcement of regulatory compliance. Protection of the enterprise data during storage as well as during transmission becomes important in order to make it consistent with the existing policies. Because of the regulatory compliance, most server resources are dedicated to single operating system and single application, hence, resources are not fully utilized. By means of virtualization, resources utilization can be increased up to 70%, which is very helpful in reducing the hardware cost as well as the power cost (Ruest and Ruest, 2009). Importance of standards and regulatory compliances in cloud computing can be further realized that some of the prominent organizations like ISACA and European Network and Information Security Agency (ENISA) (McHale, 2010) have also expressed the concern on the issue. ENISA (2011) weighing it in 123 pages have identified the most serious risks with impact factor of 7, which is highest and assigned to loss of information, compliance challenge, Risk of change of jurisdiction. Cloud computing requires to be more transparent with the efficient regulatory systems. Then only, the potential of cloud offerings can be fully realized.

This chapter is primarily focused on the software services of Cloud in the form of SaaS model. SaaS has been declared by the Software and Information Industry Association (SIIA) as a ‘tide of Web-based, outsourced products and services that remove the responsibility for installation, maintenance and upgrades from over-burdened MIS [Management Information System] staff’ (Software and Information Industry Association, 2001). This certainly has the capacity to sweep away the traditional packaged desktop and enterprise applications. A SaaS application is traditionally network based, centralized access (by the end-user) and management (by the vendor), one to many model (Ristenpart, et al., 2009). Currently, popular SaaS systems are SAP Business by Design, Microsoft Dynamics, and Google Apps. Gartner estimates that by 2012, 80% of Fortune 1000 companies will be using SaaS (Miller, 2009). Jaeger, Lin, and Grimes (2008) have explored the potential of cloud computing policy issues, while the legal issues have been discussed by Mowbray (2009). As the user is not aware about the location of the cloud resources, it poses a huge threat to the breach of privacy and safety compliance. Ristenpart et al. (2009) have discussed the vulnerabilities in the virtual machine and taken Amazon EC2 as case study. Authors have explained that it is possible to map the virtual machine infrastructure and identify the location of the machine. Such placements can