Chapter 87
Meeting Compliance Requirements While Using Cloud Services

S. Srinivasan
Texas Southern University, USA

ABSTRACT

Compliance with government and industry regulations is an essential part of conducting business in several sectors. Many of the requirements revolve around financial, privacy, or security aspects. Most of the requirements are due to federal regulations in USA while some are industry requirements that are applicable globally. Even some of the federal regulations in USA apply to service providers abroad when they are providing service to entities in USA. In that sense, all of the compliance requirements discussed here apply to a global audience. In this chapter, the authors discuss in detail the scope of the Health Insurance Portability and Accountability Act, Sarbanes-Oxley Act, Federal Information Security Management Act, Gramm-Leach-Bliley Act, Payment Card Industry Requirements, and the Statement on Auditing Standards 70. These compliance requirements concern protecting the customer data stored in the cloud with respect to confidentiality and integrity. Several of these requirements have significant enforcement powers associated with them, and businesses need to take these requirements seriously and comply. The compliance aspect involves gathering and reporting appropriate information on a regular basis. The authors present details on all these aspects in this chapter.

1. INTRODUCTION

Many businesses are required to meet certain compliance requirements either by the government or by the industry in which they operate. For many years businesses were able to gather the necessary data for compliance because they owned their IT system. With the popularity of cloud computing many businesses, both large and small which use cloud services, have to gather the necessary data in order to meet the compliance requirements. In this chapter we will identify the necessary compliance requirements and how businesses could meet those requirements with respect to some of the major laws and

DOI: 10.4018/978-1-5225-8176-5.ch087

industry requirements. These are: Health Insurance and Portability Act (HIPAA), Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Federal Information Security Management Act (FISMA), Payment Card Industry (PCI), and Statement on Auditing Standards 70 (SAS 70). These requirements are put in place to provide adequate security and privacy for the data related to financial transactions, health care records, and credit cards. Some of these laws were enacted to address the abuse of trust placed in businesses. All the requirements specified in this chapter relate to laws and requirements in USA. Because of the worldwide reach of many multinational corporations in USA many of these laws and requirements extend beyond USA and are applicable in other countries as well when they relate to businesses in USA. Thus the implications of the use of the cloud services globally have implications when it is related to an American business.

Use of cloud services by its very design leaves the control of the computing infrastructure outside the control of the business using the cloud service. Many surveys have confirmed that this lack of control is a major concern for businesses when it comes to data security. Some technologies are better suited to protecting confidential information than others. Antonopoulos and Gillam discuss many of the fundamental issues associated with cloud computing in their book (Antonopoulos, 2010). Their book provides further amplification on many of the topics discussed in this book. Information Technology is a necessary conduit to facilitate business transactions of all kinds. Today businesses gather vast amounts of data effortlessly from every type of action an individual performs with a business. Some of these data may contain confidential information related to a person's health or financial standing. The various laws and industry requirements that we will discuss in this chapter address aspects related to privacy and security of such data. In many cases the requirements involve processes and data flow aspects that businesses follow. For the cloud computing industry there is an international organization called Cloud Security Alliance (CSA) that offers guidelines and forums (Cloud Security Alliance, 2013). CSA is the leading industry supported group that provides guidelines to service providers and customers worldwide. Major corporations and government agencies that participate in CSA activities are: Amazon Web Services, Google, Microsoft, HP, Cisco, RSA, Rackspace, Oracle, US Department of Defense, and Salesforce.

Before analyzing the compliance aspects that we set out to discuss in this chapter, we discuss some of the important literature on this topic first. The growth of cloud computing is discussed in detail by Armbrust, et al in their View of Cloud Computing (Armbrust, 2010). One of the main contributions of this work is that cloud computing takes advantage of economies of scale in locating their data centers. Furthermore, many cloud providers depend on open source software since licensing models for commercial software are often a handicap for growth of cloud computing. In the influential paper "Hey, You, Get Off of My Cloud" the authors Ristenpart, Tromer, Schacham and Savage argue that the major risk in cloud computing is data co-location for multiple users. These authors recommend two ways to mitigate this risk by blocking network-based co-residence checks or a customer using all the virtual machines on a physical server irrespective of how much computing resource they need on a single server (Ristenpart, 2009). Since the growth of cloud computing is rapid, Sengupta, Kalgud and Sharma examine the security aspects in the cloud and the future research directions. Their analysis discusses the major concerns in cloud computing such as the physical security of the cloud providers' system, the way the cloud provider handles data in their servers and in backup systems, access control for the various cloud resources for the customer, and how the providers support compliance aspects (Sengupta, 2011). We conclude this brief review of current literature with the work of Yang and Tate in which they categorize the contributions of nearly 150 research articles (Yang, 2012).