Chapter 27
Cloud Environment Controls Assessment Framework

Bharat Shah
Lockheed Martin Corporation, USA

ABSTRACT

Recent years have seen the rapid growth of on-demand, flexible, low-cost cloud-based information technology services. Government and business organizations around the world have started transforming their traditional in-house data center environments to cloud-based outsourced data centers. This transformation is opening doors to new risks given that the cloud computing delivery models, related services, and technologies are still maturing and evolving. Before deployment, organizations must implement cloud environment assessment methodologies to comply with the applicable standards and regulations. They must evaluate the environment's quality attributes of Internet connectivity, user access control, privacy and confidentiality, asset protection, multiple platforms locality, availability, reliability, performance, and scalability. The purpose of this chapter is to assist organizations that are considering providing and consuming cloud-based services in developing an assessment plan specific to organizational policies, strategies and their business and applicable legal and regulatory requirements; and assessing the cloud environment controls for infrastructure, platform, and software services.

INTRODUCTION

The new wave of innovation has grown in Internet-based cloud computing in recent years. The usages of infrastructure, platforms, and software applications at large data centers through a pay-per-use leasing model have increased. Because of its ease and speed of deployment, geographic distribution capability, and financial advantages, cloud computing has emerged as one of the fastest-growing segments of the Information Technology (IT) industry. Organizations throughout the world are considering providing or consuming cloud-based application delivery models for their business growth Robinson, 2009). According to Gartner (Petty, 2010), the worldwide cloud services revenue has increased by 21.3 percent from $46.4 billion in 2008 to $58.6 billion in 2009, and the market is expected to reach $148.8 billion in 2014. cloud application services evolving from Software-as-a-Service (SaaS) offerings are poised to jump from $13.1 billion in 2008 to $40.5 billion by 2014 as business models mature.

DOI: 10.4018/978-1-4666-6539-2.ch027

The interconnectivity between cloud services makes seamless exchange of information and availability of user services any time at any place possible. This often presents unique challenges and new risks because of a lack of basic security mechanisms, especially when interconnected via a heterogeneous environment. Experience has shown that as new technologies are developed, they become a major source of new vulnerabilities and increased exposure to potential attackers. With easy-to-use and low-cost hacking tools downloadable from the Internet, attackers are capable of launching organized, disciplined, and sophisticated attacks on the cloud computing environments. The successful attacks can result in severe or catastrophic damage to the organization and nation's critical information infrastructure and ultimately threaten the nation's economy and security. In short, all information created, modified, transmitted, or received via cloud service communications must adhere to the required security goals of confidentiality, integrity, availability, sensitivity, and criticality. Organizations require a methodical approach to safeguard the cloud computing environment. Without proper safeguards, a cloud computing environment is vulnerable enabling the individuals and groups with malicious intentions to intrude and use their access to obtain and manipulate sensitive information, commit fraud, disrupt operations, or launch attacks. The objectives of this chapter are to:

- Provide an understanding of the cloud environment related services and delivery models.
- Outline benefits and challenges for deploying cloud-based service models.
- Provide the framework for assessment of cloud environment controls.

BACKGROUND

The advent of World Wide Web in the 1990s has contributed to an exponential growth in Internet-based tools and technologies. In recent years, the availability of open-source and low-cost hardware and software, and the telecommunications infrastructure has given recognition to cloud computing. The cloud concept is not new. In 1961, John McCarthy, an American computer scientist from Massachusetts Institute of Technology (Wordpress.com, 2008) had proposed a time-sharing computing model that organizations can use to sell and centrally manage computing power, hardware, software and applications like a utility (water and electricity) business models. A half a century later, cloud computing is emerging as utility-based computing that relies on Internet-based computing resources to provide services to all sizes of organizations, their business partners, and customers, while freeing them from the burden and costs of maintaining the underlying infrastructure.

Definitions

There is no one definition for cloud computing in circulation. The United States National Institute of Science and Technology (NIST) defines cloud computing as "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell, 2011).

Gartner (Petty, 2009) defines "cloud computing" as "A style of computing that characterizes a model in which providers deliver a variety of IT-enabled capabilities to consumers." Forrester (Torrens, 2008) defines "cloud computing" as "A pool of abstracted, highly scalable, and managed