ISIMC Guidelines for Secure Use of Cloud Computing by Federal Departments and Agencies

Introduction

The Federal Cloud Computing Strategy[1] outlines the Cloud First Initiative, intended to accelerate the adoption of cloud computing by federal departments and agencies, by modifying their IT portfolios to take advantage of the benefits of cloud computing to maximize capacity, improve flexibility, and minimize costs. **As stated in the strategy, "Agencies should make risk-based decisions which carefully consider the *readiness* of commercial or government providers to fulfill their Federal needs."** Cloud computing readiness considerations within the federal government include but are not limited to data security and privacy, governance and continuous monitoring. **The primary purpose of the ISIMC Guidelines is to enable federal program managers to make a careful assessment of security risks and cloud providers' *readiness* to mitigate security risks to enable the secure use of cloud computing by federal departments and agencies.**

Audience

This document is intended for CIOs, CISOs, Office of General Counsel (OGC), privacy official, designated Authorizing Officials (AO), security managers, and the program managers at federal departments and agencies who have the responsibility to assess the security impact in embracing various cloud computing models for the storage, processing, or transmission of their department or agency information.

Content

This document presents six use cases intended to help federal officials make an appropriate risk-based decision based on the cloud deployment model (Public or Private) and service model (SAAS, PAAS, or IAAS)[2]. These six use cases consider risks ranging from advanced, persistent adversaries to the increased technical complexity introduced with cloud computing. These risks and use cases are discussed through a set of "Top 20" federal cloud computing security guidelines for federal program managers and are intended to help the federal system owner to conduct their control selection based. The six use cases are identified below:

		Cloud Service Models		
		SaaS (Applications)	PaaS (APIs)	IaaS (Virtualization)
Cloud Deployment Models	Public	1. Public SaaS	2. Public PaaS	3. Public IaaS
	Private	4. Private SaaS	5. Private PaaS	6. Private IaaS

[1] Federal Cloud Computing Strategy, February 8, 2011, http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

[2] For purposes of this publication, cloud computing capabilities include infrastructure as a service (IAAS), platform as a service (PAAS), and software as a service (SAAS).