Executive Summary: Identity Management & Access Control in Cloud Computing

Recommendations and Best Practices for Using Cloud Services While Maintaining Compliance and Access Controls

ACT-IAC Cross-SIG Cloud Computing Task Group
Date Released: January 2012

Today, Federal agencies are challenged to provide enhanced levels of service in an era of restricted budgets. Adoption of cloud technologies is part of transformation in the way Government procures and operates IT systems to meet those challenges. These changes create a hybrid ecosystem consisting of a mix of Government owned, shared, and public cloud systems. The ability to effectively manage identity, credentials, and access controls to protect and govern this expanded ecosystem is an important capability to enable the rapid adoption of cloud computing.

Through case studies and leading practices this paper asserts that existing federal programs do provide the tools to enable a risk managed approach to achieve Federal goals around cloud computing adoption.

This drive towards transparency and consolidation of IT has led to the recognition of several important drivers that are currently impacting Federal Agency Chief Information Officers:

1) the drive for workplace mobility and collaboration through improved implementation of Identity and Access Management (IAM) and utilization of smartcard credentials for access to Federal and commercial computer systems

2) the drive for Federal Agencies to decrease the infrastructure footprint (both data center and workplace) from an economic and environmental standpoint through utilization of cloud computing for cost effective delivery and consumption of IT services to their internal and external constituents

3) the drive for increased security and defence against an increasing cybersecurity threat

4) the cultural change of moving from dedicated Government owned IT systems to a hybrid ecosystem consisting of a mix of Government owned, shared, and public cloud systems

Some have expressed concerns that these drivers are inherently in conflict with each other. While the initiatives have great value, there are concerns that agencies will resolve the apparent conflict by slowing their adoption of cloud computing. The result of this approach will be a significant limitation in the ability of Federal Agencies to realize the benefits associated with the cloud computing model. The ability to effectively manage identity, credentials and access controls to protect and govern this expanded ecosystem, while presenting some challenges, is an important capability to enable the rapid adoption of cloud computing.

The goal of this paper is to analyze the relationships between these drivers and to provide recommendations to Federal Agencies on how to effectively address both of them in a manner that allows agencies to comply with IAM mandates and embrace the emerging cloud computing paradigm.

Access Control Models There are two basic models for access control; authentication based access control starts with a user credential and then expects the service provider to honor that credential,
authentication based access control accepts that services are written to accept a specified set of credentials and then expects the user credential to map to one of these. Authentication based models work well if the credential owning organization owns or controls the service a user wishes to access, such as Government users accessing Government systems. Authorization based models work best when the credential owning organization does not own or control the service to be accessed, but wants to facilitate access by their users in a controlled way. For this paper, which focuses on Government use of externally hosted services, authorization based access control models represent best practice.

Challenges and Best Practices Specific challenges exist around compliance with Federal IAM regulation and policy, protection of information in the cloud, IAM differences between the NIST service models (Infrastructure, Platform, and Software as a Service), the ability to use and trust external credentials, and the management and governance of IAM in a cloud context. Each challenge is discussed and can be addressed within the context of existing FICAM related programs and best practices.

FICAM, NIST and NSTIC Enable Cloud Adoption The Federal Identity, Credential and Access Management (FICAM) establish an architecture, roadmap, and implementation guidance for Federal Agencies. This is structured around five areas: identity, credentials, access control, federation, and auditing/reporting needs. The OMB M-11-11 mandate and FICAM do not represent barriers to the use of cloud computing. In fact, the implementation of FICAM by Agencies will improve their ability to leverage cloud-based services from multiple providers. The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a program that encourages commercial adoption of trusted identity, credentials, and access management best practices. Increasing adoption of trusted credentials by commercial providers supports secure, risk managed access to commercial cloud services. NIST has been tasked by the Federal CIO to accelerate the adoption of secure and effective cloud computing by Federal Agencies. The NIST cloud computing program has developed Special Publications that define and support the adoption of cloud computing standards and best practices.

Case Studies and Recommendations A number of case studies are presented that demonstrate how agencies have addressed IAM in their cloud programs. Specific recommendations are presented for improving the federal IAM programs to facilitate and clarify issues around cloud adoption by Government.

The Bottom Line is that, while there are challenges to IAM in the cloud, existing federal programs do provide the tools to enable a risk managed approach to achieve Federal goals around cloud computing adoption.

Copyright ©American Council for Technology, 2012. This document may be quoted, reproduced and/or distributed without permission provided that credit is given to the American Council for Technology and Industry Advisory Council.

For further information, contact the American Council for Technology- Industry Advisory Council at (703) 208-4800 or www.actgov.org.