HARVARD UNIVERSITY

Enterprise Architecture
Harvard University Information Technology

HUIT Standard

AWS Account Management

Authors: • Sevier, Raoul • Charest, Greg	**Audience Level:** • IT Director / Manager • Solution Architect and Project Manager • Application Developer and Designer • DevOps Staff
Version: 1.01 **Last Revised:** 8/10/2020 2:53:00 PM **Status:** Published **Document Type:** Single Topic Advisory	**Distribution Scope:** • HUIT
Workgroup Members:	**Reviewers:** • Burson, Jefferson – EA • Frazier, Ryan - HBS • Larsen, Tamara- DevOps • Mabbott, Tim – HBS • Mulvey, Jim - HBS • Rogers, Chris - SEAS • Rota, Ben – Cloud Consulting • Vaverchak, Tim – Shared Services

Document Change Log

Date	Editor	Changes
12-Jun-2020	Raoul Sevier	Initial Draft
19-Jun-2020	Greg Charest	Draft revisions
02-Jul-2020	Greg Charest	Revised based on feedback
02-Jul-2020	Raoul Sevier	Draft revisions
13-Jul-2020	Raoul Sevier	Final pre-RFC adjustments
20-Jul-2020	Raoul Sevier	Pre-RFC feedback incorporated and RFC version released
30-Jul-2020	Raoul Sevier	Published version 1.0

1. Problem Statement

Effective management of cloud-based IT infrastructure and costs in a large research university with a decentralized culture requires local control and decision making. However, without adequate visibility and control mechanisms at the university level, decentralized IT procurement and management can lead to a lack of accountability and lower economies of scale.

AWS account management and billing is fairly centralized within Harvard, but not completely so. The centralized approach has significant benefits to both HUIT and the University, but additional local account management capability would allow School partners to better manage their AWS costs and security requirements. A number of Schools have requested access to the AWS Organizations service in order to improve local account management.

2. Recommendations

1. Move to a limited multi-payer design necessary to use the AWS Organizations service in order to support HUIT partner and Cloud Shield 2.0 requirements.
2. Document a process for creating a limited number of additional self-service AWS 'payer' accounts that includes approval criteria and specific mitigations to protect University enterprise level interests.
3. Require the use of HUIT centralized billing for all Harvard AWS services.
4. Define and adopt security policies and practices related to payer accounts and the use of AWS Organizations to further enhance cloud security.

3. Discussion

The design of the AWS payers model has several considerations, detailed below.

3.1. Single Payer Design

HUIT currently has a very limited the number of AWS payers[1] with most accounts under the HUIT Payer and the General Payer.

The use of a predominantly single payer approach has the following benefits:

- Annual Harvard AWS spend is easily ascertained
- Enterprise Support costs can be efficiently recovered via the centralized billing process

[1] Two groups, HBP and DCE, have existing Payers that pre-date the creation of the current structure. In addition, a single exception has been given for FISMA compliance.

- Time and effort costs associated with adding new payers are avoided
- Individual AWS accounts represent billing and accountability boundaries
- Security and risk management accountability is clear

The disadvantage of this centralized single payer approach is that it limits the ability of local Harvard IT organizations to manage their own AWS accounts. Specifically, it prevents them from using the policy and account management tools available through the AWS Organizations service, and other associated technologies such as AWS Control Tower. This is because the root or top level in an Organization must be a payer account and there is no mechanism for the delegation of important administrative functions to sub-organizational units.

3.2. Multi Payer Design

The use of multiple AWS payer accounts would support a more distributed management and control model. Using a dedicated payer account, various Harvard organizations would have greater control over local linked accounts and would be able to take advantage of the policy and account management tools available through the AWS Organizations service.

The drawbacks of a multi-payer model include:

- Additional expenses associated with updating AWS support, discount and data egress waivers for each new payer account
- A reduction of University level visibility into total AWS spend resulting in additional effort to ensure we are meeting contractual commitments
- Potential loss of billing efficiency due to duplication of billing systems
- Additional effort to establish and monitor security compliance

3.3. Partner Access to the AWS Organizations Service

HUIT partners would like to have local ability to:

- Create organization units (OUs) and apply group policies to more effectively manage sub-organizational account
- Log to their own infrastructure
- Enforce additional security controls as needed
- Manage costs across accounts
- Vend[2] accounts

Amazon now offers AWS Organizations, an account management service that enables the consolidation of multiple AWS accounts into centrally managed groups. AWS Organizations

[2] Vending occurs when organizations further delegate portions of their accounts, with some autonomy, to subsidiary organizations.

includes account management and consolidated billing capabilities to support budgetary, security, and compliance requirements.

The use of the AWS Organizations service would support the key requirement of creating and managing OUs[3] but would also require a shift from a primarily single payer strategy to a multi-payer strategy to support the creation of root level organizational structures for Partner organizations.

3.4. Billing Considerations

Centralized billing is important for the following reasons:

- Enterprise cost visibility and monitoring
- Efficiency
- Financial management
- As a mechanism for cost recovery

4. Recommended Design

Any solution must meet the following criteria:

- All participating Harvard organizations should maintain access to Enterprise Support, the Enterprise Discount, the Data Egress Waiver and centralized billing.
- Key benefits of the single payer approach should be maintained to the extent possible or be effectively remediated
- Local control and overall security levels should be enhanced

A limited multi-payer model, using AWS Organizations and specific mitigation policies represents a balanced and effective approach and can meet the above criteria. Because the creation of additional payers results in added costs and complexity, the number of additional payer accounts should be limited and each addition should be carefully evaluated to balance costs and benefits.

The following specific policies should be implemented with a limited multi-payer model:

Visibility:

- All payers must maintain an AWS role for HUIT Finance
- HUIT will pay all bills and rebill through the GL when Finance completes the interface

Billing:

- A default GL must be provided for use if no other one is specified

Security:

- Root credentials for the Payer must be escrowed with HUIT, except where required by compliance regimes such as FISMA

[3] Other requirements can be met without using Organizations

- A “Break glass” role for InfoSec must be maintained
- The owner of the Payer account will be accountable for all activity in subaccounts (for audit purposes)
- The Payer must be managed by a professional IT team with AWS experience and a dedicated Cloud team

Operations & Administration:

- New Payers must provide a justification based on
  - A compliance exception. e.g FISMA
  - A documented need to manage multiple policies/sub-accounts
- All exceptions must be formally requested of and approved by HUIT CTO or CIO

5. Compliance

HUIT will continue to be the focal point for account, payer, and organization relationships with AWS. Over time, constructs such as AWS accounts, GL codes, and organizations will need to keep abreast of changes in technologies and usage.

5.1. New Payers

The Cloud Community of Practice (Cloud CoP) and the Architecture Review Group (ARG) are venues for discussion and consideration for potential new Payers.

5.2. Updates

Schools, other organizations, and HUIT will use existing communications channels to convey issues, constraints, and new requirements. As necessary, unresolved issues can be presented to existing forums such as the CIO Council.

6. References

- AWS Organizations - The Case for Change
  - Refer to the Enterprise Architecture web site:
    - https://enterprisearchitecture.harvard.edu