



Vermont Enterprise Architecture Framework (VEAF)

Identity & Access Management (IAM)

Abridged Strategy

Level 0

EA APPROVALS

EA Approving Authority:

<Signature>	<Date>
<Printed Name>	<Position Title>

Revision History

Version	Date	Organization/Point of Contact	Description of Changes
0.1	12/15/2013	Chad Scott, Jay Mason, Cameron Bradley	Primary content authors, edited to create
	9/21/2015	CTO, John P Hunt	Final draft for strategic discussions.

Confidentiality Statement

This document is produced for the Vermont Health Connect (VHC) and cannot be reproduced or distributed to any third party without prior written consent.

No part of this document may be modified, deleted, or expanded by any process or means without prior written permission from the State of Vermont.

Table of Contents

1	Identity & Access Management Executive Overview	4
1.1	Purpose	4
1.2	Value of IAM	4
2	Identity & Access Management Strategic Principles	5
2.1	Information Access Management Standards	5
2.1.1	NIST Standards	6
2.1.2	Privacy	6
2.2	Best Practices	6
3	Maturity Matrices & Roadmap	7
3.1	Maturity of IAM Architecture	7
3.2	IAM Roadmap	8
4	IAM Center of Excellence	9

Table of Figures

Figure 1	IAM Roadmap	8
----------	-------------	---

Table of Tables

Table 1	IAM Maturity Levels	7
---------	---------------------	---

1 Identity & Access Management Executive Overview

1.1 Purpose

The purpose of this document is to describe the overall concept and strategy for Identity and Access Management (IAM).

Audience – The intended audience for this document is State Executives, Enterprise and Business Architects, and Business Analysts attempting to enable IAM within their business units.

1.2 Value of IAM

IAM components increase security and decrease the potential for identity theft, data breaches, and trust violations. These support compliance with Federal and State rules, regulations and standards.

IAM lowers cost for user management, automating business processes, providing better security through centralized policies, and reducing risk by creating auditable records of changes to user accounts and access policies. IAM components are capable of creating a single authoritative record of an individual that can be referenced by all appropriate SoV systems.

The capabilities provided by IAM architecture fall into the following four main categories:

- **Identity Management:** Involves the creation of user accounts, their maintenance, and removal. At any given time, an administrator can find all users for a given system, which systems a given user can access, their permissions within each system.
- **Access Management:** Determines what resources users can access. Access Management controls the user authentication process, provides Single Sign-On (SSO), and multi-factor authentication (MFA) functionality across SoV systems.
- **Directory Services:** A central repository for all user accounts; used by other services to obtain information about a user within State applications using IAM. The central user repository contains acts as a single point of truth for the user.
- **Centralized Administration:** Centralized administration that creates an audit trail for all user account changes. Administrators can know and attest to all systems and resources that a given user has access to at any time. Workflows that implement a separation of duties, require that permission changes must first be approved by the appropriate authority.

The current state of IAM at the State has multiple departments using their own IAM solutions this, while advancing awareness of IAM at the departmental level, is not an effective use of SoV IT resources. These solutions are small and disconnected, apply unique sets of standards and practices, and often produce their own user directories with little or no connection to State strategies.

IAM supports the following business objectives:

- Allow users to quickly obtain access to the systems needed to do their jobs
- Transition from a manually intensive, non-centralized process
- Provide a clear and immediate visibility into who has access to what systems
- Provide an efficient means to create, deliver, and maintain user accounts and permissions
- Meet compliance and regulatory requirements
- Provide an auditing mechanism to track user account changes and system access

2 Identity & Access Management Strategic Principles

The key strategic principles for IAM are as follows:

- Initiatives must be driven by priorities and requirements
- Implementations must be viewed with an enterprise-wide perspective
 - All stakeholders must be included in IAM discussions
 - Programs and policies must be socialized across the enterprise
- Solutions should prioritize configuration and avoid customization
 - Solutions should reduce complexity and increase efficiency
- Proactively assess the success of the Identity & Access Management solutions

2.1 Information Access Management Standards

DII's vision is to use a common IAM framework across all State agencies and functional areas. An IAM solution must be extensible as the State must account for multiple best practices and requirements specific to target areas, including, but not limited to Federal Tax Information (FTI) and Personal Health Information (PHI).

2.1.1 NIST Standards

The National Institute of Standards and Technology (NIST) 800 series standards, specifically NIST 800-53 and 800-63, are of key importance to the IAM strategy of the State of Vermont. They reach into several target areas, such as the IRS 1075 requirements for Tax systems, they also have significant overlap with ISO 27001 controls.

Areas of the NIST 800 series standards that apply directly to the State’s IAM strategy are:

- **Access Control**
 - Management, enforcement, separation of duties
- **Audit and Accountability**
 - Auditable events, audit reduction, and report generation
- **Identification and Authentication**
 - Identifier and Authenticator Management

2.1.2 Privacy

Due to the diversified nature of State agencies, an all-encompassing State IAM strategy must consider a number of diverse privacy standards in addition to the NIST 800 Series. State of Vermont IAM solutions must accommodate the privacy needs of a wide variety of areas (where applicable) such as:

- HIPAA (Agency of Human Services)
- FERPA (Department of Education, Vermont State Colleges)
- IRS 1075 (Department of Tax)
- Personally Identifiable Information (PII)

2.2 Best Practices

After implementation all user account creation and administration should be performed using IAM. From IAM, new accounts are provisioned and changes are propagated to the SoV systems for which the user is granted access. Proper administration of IAM is critical to the performance of all systems using IAM, and it is likewise critical to apply best practices in order to avoid problems that are both time-consuming and costly to correct.

The following IAM best practices should be followed at all times:

- Grant least privilege
 - Users should only have the minimum access to perform their job function
- Manage users via group
 - Managing groups is more efficient than managing individual users
- Consider security, and create strong password policies
- Regularly audit users and remove access to unused user accounts

3 Maturity Matrices & Roadmap

3.1 Maturity of IAM Architecture

The State of Vermont has only begun the implementation of centralized IAM for the Health Services Enterprise Platform (HSEP), and is only in the early stages of its maturity. As a rule, organizations move only advance through one maturity level at a time via an iterative process. DII is advising the utilization of infrastructure as a service (IaaS) to enable this transition.

The maturity of the current state of IAM and its implementation is depicted in the figure below.

Table 1 IAM Maturity Levels

	Initial	Developing	Defined	Managed	Optimized
Governance	Ad Hoc	Submersed into InfoSec	IAM governance Structure defined and accepted	IAM governance structure fulfilled and refined	IAM governance optimized
Organization	Informational basic roles and responsibilities are decentralized	Technical projects sponsored by the business and Chief Information Security Officer (CISO)	IAM PMO established, IAM roles and training needs defined	IAM PMO active; RACI matrix defined, proactive skill development	Optimal integration with business; skills optimized
Vision and Strategy	Conceptual awareness	Business drivers identified and tactical priorities set	Business-aligned vision defined: strategic priorities set	IAM vision and strategy continually reviewed to track business strategy	Periodic optimization of vision and strategy
Processes	Ad Hoc	Semi-formal Business Unit, and target specific processes.	Formal process defined, consistent across the Bus and target systems	Formal process integrated and refined; aligned with business process	Process optimization
Architecture and Infrastructure Design	Possible use of target specific productivity issues	Disjointed technical projects: technology redundancy is likely	Discrete architecture defined: rationalization and consolidation in hand	IAM Architecture refined and aligned with EA	IAM architecture imbedded within EA; optimized
Business Value	Non measurable	Technical efficiency and effectiveness improvements: low direct value	Sustained quantifiable improvements tied to GRC imperatives	Sustained quantifiable to all key business imperatives; high direct value	Business value optimization; transformational direct value

Governance: Currently there are a number of regulations that the State must comply with due to the sensitive nature of the content that it manages. They include but are not limited to HIPAA, NIST SP800-53, FERPA, IRS 1075, and Personally Identifiable Information (PII) controls. However, these are only used as required, there is no governance in place across the enterprise.

Vision and Strategy: At this point certain business drivers have been identified, and tactical priorities have been set.

Processes: All process are ad hoc, there are no formal processes in place for the State as a whole.

Organization: Organizationally there are defined roles that can add users, modify user groups, and user roles. The current structure does not have a hierarchical organization structure necessary to provide the IAM system with defined managers and approvers for future workflows.

Architecture and Infrastructure Design: An architecture based on strategy has been developed.

Business Value: As the maturity of the IAM solution is developed, the business value should grow and be more easily measured. It is critical that the IAM solution be aligned with business needs.

3.2 IAM Roadmap

Improving the maturity of the IAM architecture will require numerous stages to expand and improve the services. Figure 5 below demonstrates some of the next steps in achieving that maturation.

Transition Roadmap

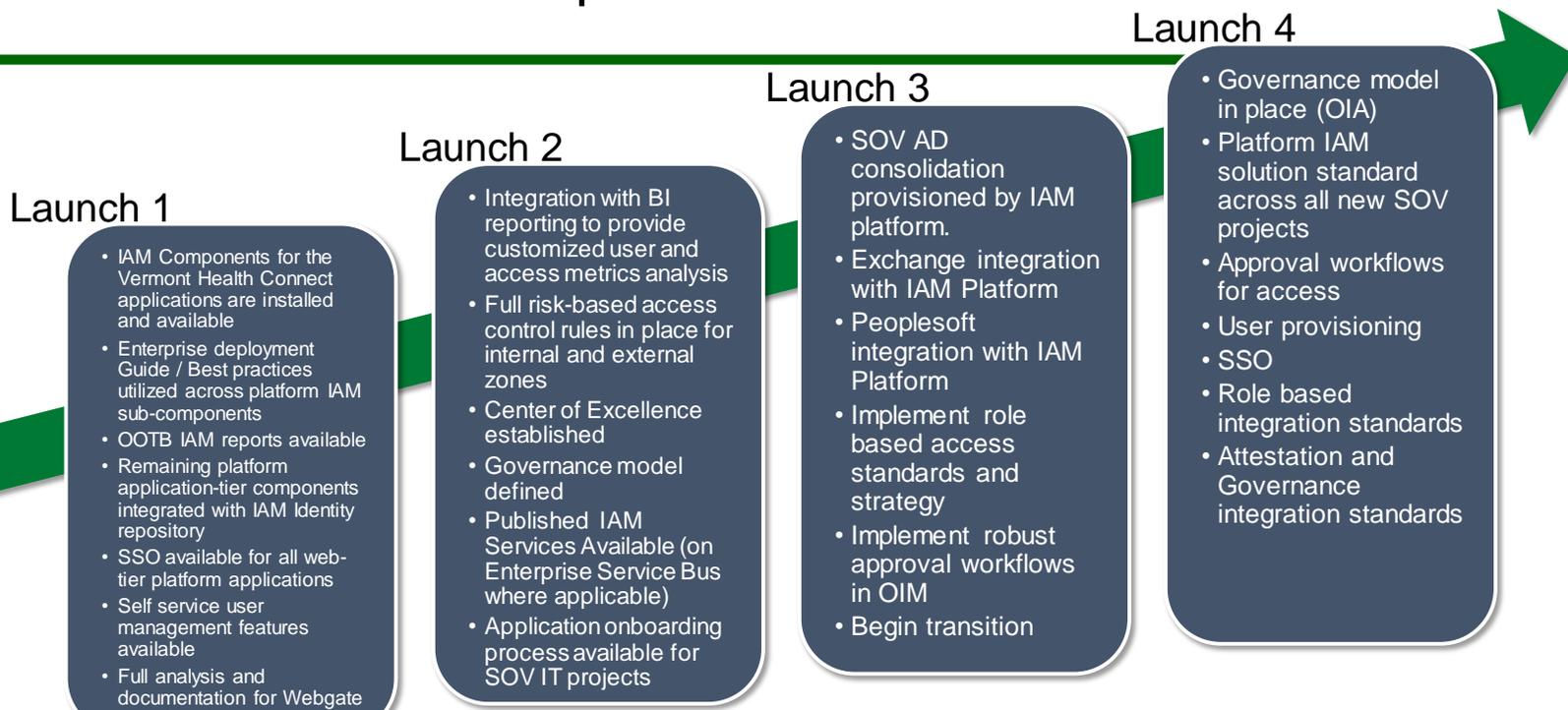


Figure 1 IAM Roadmap

4 IAM Center of Excellence

An IAM Center of Excellence (CoE) will leverage limited staff with specialized skills to align with business users and deliver against the strategy, guiding principles, and best practices. A CoE is more effective than having multiple individual IAM teams for each project.

The IAM CoE should be comprised of Enterprise Architects who have a good understanding of IAM best practices, have hands-on experience with the Oracle IAM Suite, and can relate this understanding and experience to State application implementation teams and the business.

The SOV IAM Platform is intended to eliminate silos of application and department specific user repositories. Without centralized authority, small departmental solutions will remain disconnected from larger strategies.

IAM touches all areas of the enterprise architecture. Without a clear lines of responsibility, IAM will be inconsistent and inefficient, resulting in delayed response to the resolution of user issues.

The major benefits for establishing the enterprise IAM CoE include:

- Alignment between business and IT
- More efficient use of resources
- Drive overall adoption of user provisioning, directory, and access management services
- Provide a standardized, sustainable, and scalable enterprise wide environment

The overarching goal of a strong centralized IAM CoE should be to promote “self-service” in the user community in a secure and controlled manner.

The role of the IAM CoE will be to govern and execute IAM across the enterprise with specific concentration toward the following tasks:

- Standardization
- Training and Education
- Continuous Process Improvement
- Best Practices definition and promotion
- IAM Project oversight and management
- Platform Architecture
- Directory Architecture
- Data Quality (In conjunction with the MDM CoE)
- Centralized Support and Vendor Relationships
- Standard Application Provisioning Processes
- Application Platform Administration