Identity and Access Management
Identity Data Stewardship Committee

Revised on November 8, 2013

Objective

To advance the data governance mission of the University, the Identity and Access Management (IAM) Program will work in partnership with the Identity Data Stewardship committee to provide a strategic foundation for continuous identity data quality improvement, identity data governance and role governance. It is essential for Yale to implement a cohesive Identity Data Stewardship Committee that enables the involvement of the Identity Owners, General Counsel, Provost and HIPAA Office and Role Owners. This committee will be undertaken as a collaborative effort across the University to ensure all the identity data authoritative systems are used for the Identity and Access Management Enterprise Directory. In addition, this committee will be the governing body to ensure University-wide standardization of roles.

Responsibilities

This committee will meet on a regular basis to review authoritative systems, identity data issues, role modeling scope, approvals, progress and prioritization. This group may also be asked to meet on an ad hoc basis to weigh in on decisions needed on the IAM Program.

Identity Data Governance:

- Support IAM Program’s on-going identity data profiling activities and help resolve issues with authoritative systems
- Help identify authoritative system for each identity data element (staff, faculty, students, alumni)
- Help drive opportunities for identity optimization throughout the University
- Guidance on regulatory, privacy & access issues, Policies & Procedures, Standard
- Support IAM effort’s identity data cleanup efforts, in alignment with the University’s goal of Data Clean-up
- ‘Own’ the University Identity Data Model
- Task the authoritative systems’ development teams to change when needed
- Help IAM ensure that Identity data is:
  - Accurate, complete, timely, and relevant for the intended purpose;
  - Collected, maintained, used, and disseminated in a way that respects privacy and ensures confidentiality and security

Members

Co-Chair: Liz Burnell, Director of Identity & Access Management (Functional)

Co-Chair: Josh Nabozny, Director of Identity & Access Management (ISO)

Nancy Creel-Gross, Senior Director Human Resources

Julie Grant, Assistant VP BUSOPS Business Operations

Steve Murphy, AVP Finance & University Controller

Jackie Tucker, Senior Director, Business Solutions

Susan Bourey, HIPAA Privacy Officer, Human Research Protection Program

Jenny Chavira, Deputy Executive Director Association of Yale Alumni

OPEN – Development

Judy Offutt, Associate Director Human Resources Information Systems

Gabriel Olszewski, Registrar

Diane Rodrigues, Director, Office of Faculty Administrative Services

Harold Rose, Senior Associate General Counsel, Office of the General Counsel

Lloyd Suttle, Deputy Provost for Academic Resources

Yale Information Technology Services
Identity and Access Management
Identity Data Stewardship Committee

Revised on November 8, 2013

• Meet the goals of assuring accuracy to ensure that decisions are based on the best possible information.

Role Governance
Role-based access control (RBAC) is becoming the standard for managing entitlements within systems and applications. RBAC will play a significant part in establishing a model for enforcing security within applications. In addition, it is a critical component of the Identity & Access Management (IAM) framework. It essentially simplifies entitlement management by using roles, as opposed to users, as authorization subjects.

Role engineering is the process of defining roles and related information, such as permissions, constraints and role hierarchies, as they pertain to the users’ functional use of systems, applications and business processes. It is a critical step in deploying RBAC-oriented IAM systems.

Benefits:
This will benefit the University by reducing the risk of users having inappropriate access privileges and aggregating entitlements as they change job functions within the University. As the users change their job function, they are assigned new roles and old roles are removed from their profile. This results in users’ entitlements matching their job functions.

With the emergence of various regulatory requirements, such as, Health Insurance Portability and Accountability Act (HIPAA), it is increasingly important to streamline the entitlement management process with business oversight, as it has become a security governance and compliance issue.

Standardize the use of roles across critical systems at the University.

Simplify user access provisioning and de-commissioning.

RBAC has proven to be cost-effective for reducing entitlement management costs and complexity

Responsibilities:
• Governing body for Role Governance across the University
• Support the Role Modeling projects and help resolve any issues escalated during the process
  • Be accountable for the scope identified in each role modeling

Cynthia Smith, Associate Provost for Health Affairs and Academic Integrity
Judith Calvert, Assistant Dean & Registrar Law School
Anna Maria Hummerstone, Director of Human Resources for Yale School of Medicine
Millie Anderson, Supervisor Yale School of Medicine Finance
Patrick McMorran, IT Support Tech School of Architecture

Meeting Frequency
Monthly and Ad Hoc as needed

Yale Information Technology Services
IDENTITY AND ACCESS MANAGEMENT
IDENTITY DATA STEWARDSHIP COMMITTEE

Revised on November 8, 2013

- Help drive opportunities for role standardization throughout the University
- Guidance on regulatory, privacy & access issues, Policies & Procedures, Standard as they relate to role risk models

Composition
As a team, the members of the Identity Data Stewardship Committee should demonstrate
- Diversity of disciplinary backgrounds
- Varied perspectives
- Professional courtesy
- Willingness to engage and transform.

IAM Staff Responsibilities
The Identity and Access Management staff will provide the following support to the committee
- Agenda generation, preparation and distribution; meeting notes preparation and distribution
- Identity Data Quality Issue Management Process
- Miscellaneous activities
- Task tracking and reminders.
- Role Modeling Projects, stats, issue tracking