Identity & Access Management, Managed Services, Custom Application Development and Data Center Solutions

IAM Open Discussion

Todd Rossin
Managing Director
610.329.3276
todd@idmworks.com

Leave it to us
Who is IDMWORKS

- Operational Since 2004
- Privately Owned
- Recognized by Gartner as one of the Top 10 IAM Consultancies in North America
- 60+ Consultants
- Proven methodology & approach, 95% of employees are US Citizens, 100% are W2, 25% have US Government security clearances, each consultant has an average of +5 years experience in Identity and Access Management, & our consultants are located throughout North America
- Vendor Partnerships with: Aveksa, Axiomatics, Avatier, CA, Courion, CyberArk, FoxT, Hitachi, IBM, Microsoft, NetIQ (Novell), Oracle (includes legacy Sun & Passlogix), PingIdentity, Quest (Dell), RSA & SailPoint
- Hundreds of Successful Engagement with Clients Across Multiple Sectors
Health Care: Dignity Health, Health First, Catholic Healthcare West, Children’s Hospital of Philadelphia (CHOP), Priority Health, Excellus BCBS, Wellmark BCBS, Kaiser Permanente, Horizon BCBS, BCBS Michigan, Carefirst BCBS, Cincinnati Children’s, Unitrin, Guardian, Select Medical, Center for Medicare & Medicaid, United Health Group, GlaxoSmithKline, Baylor Health Group, Lawrence Livermore National Laboratory

Utilities: ERCOT, Pennsylvania Power & Light, We Energies, Midwest ISO, UTi


State & Local: NYDOH, Hennepin County

Higher Education: West Virginia U, Ithaca College, City University of New York, U of Massachusetts, Embry-Riddle Aeronautical University, Widener College, Coppin State College, Syracuse U, Ohio State U, Northland College

Financial: Alliance Data, TD Bank N.A., Freddie Mac, Woodforest National Bank, Northern Trust Bank, ITT, Capital One, M&T Bank, MBNA, Great American Financial, JPMC

Commercial: General Motors, Lowes, Holland America Line, Carmax, Subaru of America, AAA, Freightliner, Condé Nast, Gartner, Paychex, Tyco Electronics, Toyota Motor Sales, Dell, AON, Towers Perrin, Rohn & Haas, Rockwell Automation, McDonalds Corp, Oppenheimer Funds, Nike
IDMWORKS is one of the top ten Identity and Access Management: IAM consultancies in the US with extensive experience helping clients solve challenges across all IAM disciplines and vendor technologies:
What is Identity and Access Management?
Gartner Definitions of the IAM Space

• Assessment & Roadmap - Review and Planning
• User Provisioning - Automation of user management and access to systems within an organization
• Change Management - Automation and support for development, rollout and maintenance of system components from current state to future state
• Role LifeCycle Management - Modeling and implementation of Roles within an organization
• Access Management - Real-time enforcement of application security using identity-based controls and provisioned access rights
• Governance - Implementation of a controls based framework and a robust governance program
• Audit & Compliance - Support for laws, regulation and policies defined within an organization for Business and IT
Success Approach

• Validate your current state
• Highlight your constraints
• Identify your crucial success factors
• Define your desired state & first win
• Develop your blueprint
• Deliver a step by step roadmap:
  ▪ Costs
  ▪ Timelines
  ▪ Milestones
  ▪ Business Justification
Product Areas of the IAM Space

- Provisioning & Password Mgt
- Access Control
- Access Governance
- Single Sign-On & Federation
- Privileged User Management
Provisioning & Password Management

- Trouble Ticket System
- Spreadsheet
- Emails

- Human Resources
- Active Directory
- Applications
- Applications
- Applications

Employee

Add

Moves

Deletes
Provisioning & Password Management

Trouble Ticket System

Spread-sheet

Emails

Reports & Audits

Reports & Audits

Reports & Audits

Employee Adds Moves Deletes

Human Resources

Active Directory

Applications

Applications

Applications

Manual System Requires Multi-Steps Takes Weeks or Months No Audit Trail
Provisioning & Password Management

Provisioning & Password Mgt
Identity Management System

Human Resources
Active Directory
Applications
Applications
Applications

Automated System
Self Service System
Real-time
Includes Audit Trail

Employee
Adds
Moves
Deletes

Reports & Audits

ORACLE
NETIQ
DELL/QUEST
COURION
MICROSOFT
CA
IBM
AVATIER
AVEKSA
SAILPOINT
✓ Assess environment and interview stakeholders to find gaps in “as-is” and “should-be” states
✓ Form a team of business owners, IT Sec, audit and compliance
✓ Focus on workflow and narrow the initial goal:
  o Human or non-human
  o Address mobile environment (BYOD)
  o Areas that can be improved quickly
✓ Gain Executive buy-in for funding by focusing on gains:
  o Automate the account process: new, change, & remove for efficiency
  o Improved speed to onboard
  o Improve security on entitlement creep
  o Improved audit on off-boarding
  o Speed to deliver audit data
Validating Access Entitlements

Access Control

Human Resources
Active Directory
Applications
Applications
Applications

Employ Adds
Moves Deletes

RBAC: Create Role
ABAC: Define Attributes
PBAC: Create Policies
Automate Access
Single Sign-On

Reports & Audits
Reports & Audits
Reports & Audits
Validating Access Entitlements

Access Control
- Employee Adds
- Moves
- Deletes

Access Governance
- Reports & Audits

Human Resources
- Active Directory
- Applications

Automated Validation of Entitlements
Attestation
Automated Audit
Validating Access Entitlements

Provisioning & Password Mgt
Identity Management System

Access Control & Governance
AGS System

Human Resources
Active Directory
Applications

ORACLE
NETIQ
DELL/QUEST
COURION
IBM
CA
AVATIER
SAILPOINT
AVEKSA
AXIOMATICS

Automated Changes
Real-Time
1) Policy Enforcement
2) Management Approvals
3) Audit Trail

© 2013 IDMWORKS
✓ Assess environment and interview stakeholders to find key applications that require automation for improved compliance

✓ Form another team of business owners & IT Sec to define the ideal user experience (employee and manager)

✓ Review organizational goals around user accounts:
  - RBAC
  - ABAC
  - PBAC

✓ Automate the process, then look for the orphans and exceptions

✓ Focus on:
  - Speed to respond and remediate audit findings
  - Automation of manual audit response process
  - Address mobile environment (BYOD)
Access to External Applications

- Every Application Requires Integration to Every External Application for Access
- Employee Adds, Moves, Deletes
- System Adds, Moves, Deletes
- Applications
- Applications
- Applications
- No Common Control
- No Audit
- Emails
- Trouble Ticket System
- Spreadsheet
Access to External Applications

- System: Adds, Moves, Deletes
- Employee: Adds, Moves, Deletes
- Single Sign-On & Federation
- Applications
- Centralized Security
- Policy Enforcement
- Complete Audit Trail
- ORACLE
- NETIQ
- CA
- DELL/QUEST
- MICROSOFT
- PINGIDENTITY
- IBM
Voice of Experience

- Focus on the client
  - Employee satisfaction around SSO
  - Customer / Partner integration (ease of doing business)
- Assess the number of SAS connections and pick two for early federation to use as a use case for standard approach
- Consider human and non-human systems integration
- Tie project with cloud initiatives
  - HR
  - CRM
  - Supply chain
Privileged User Access

In addition to System Admins, Dbase Admins, Server Admins & Infra Admins ... Every Non Human Applications Have Access to Systems Which Requires Manual Development & Audit

Everyone Has Same Access
No Audit
Privileged User Access

Can Filter Access
Log Usage & Record Suspicious Activity
Audit
Form a team of IT Sec, development & audit and compliance to define the approach to control “superuser” access

Assess your current state and define gaps to desired state

Implement a Privileged User/Account/Access Management Solution

Automate the process, then look for the orphans and exceptions
Vendors (not all, but most)

Provisioning & Password Mgt
- ORACLE
- NETIQ
- CA
- IBM
- DELL/QUEST
- COURION
- MICROSOFT
- AVATIER
- SAILPOINT
- AVEKSA

Access Control
- ORACLE
- NETIQ
- CA
- DELL/QUEST
- COURION
- IBM
- AVATIER
- SAILPOINT
- AVEKSA
- AXIOMATIC

Access Governance
- ORACLE
- NETIQ
- CA
- DELL/QUEST
- COURION
- IBM
- AVATIER
- SAILPOINT
- AVEKSA
- MICROSOFT
- PINGIDENTITY
- IBM

Single Sign-On & Federation
- ORACLE
- NETIQ
- CA
- DELL/QUEST
- COURION
- IBM
- AVATIER
- SAILPOINT
- AVEKSA
- MICROSOFT
- PINGIDENTITY
- IBM

Privileged User Management
- ORACLE
- DELL/QUEST
- CYBERARK
Client Case Study: Provisioning

- 60,000 employee Healthcare Provider
- Operating forty facilities throughout CA, NV & AZ
- 6000 employee changes per month (was manual & batch processing)
- Legacy IdM environment migrated to new provisioning platform
- Centralized authentication & authorization
  - Identified most critical applications
  - Automated access to top 25 application with plan for +400 other applications
  - Improved audit compliance requirements
Client Case Study: Access Governance

- 8700 employees operating in 70 countries with numerous remote users
- Largest independent provider of insurance claims management solutions for risk and insurance industry
- Access Governance project
  - Initial quick start didn’t produce fully functional system
  - Tied role management to provisioning
  - Access rights can be de-provisioned real-time
  - Automated logging & reporting for compliance
Client Case Study: Single Sign-on & Federation

- 44000 employee apparel manufacturer & retailer operating worldwide
- Huge supply chain network with numerous SAS connections
- Trusted partners in the US and overseas
- Federated identity and Federated single sign-on needs addressed
- Automated logging and reporting for compliance
Key Questions

• Who are the key stakeholders in your IAM project(s)?
• How are you communicating cost benefits of your identity and access management system(s)?
• Have you assessed the following:
  ▪ Automated Provisioning
  ▪ Password Management
  ▪ Access Governance
  ▪ Single Sign-On & Federation
  ▪ Privileged User Access Management
• How are you maintaining and improving IAM systems?
• How are you working with audit and compliance?
Assessment Approach

• Validate your current state
• Highlight your constraints
• Identify your crucial success factors
• Define your desired state & first win
• Develop your blueprint
• Deliver a step by step roadmap:
  ▪ Costs
  ▪ Timelines
  ▪ Milestones
  ▪ Business Justification