Identity Access Management - Challenges and Best Practices

Mr. Todd Rossin, Managing Director/Founder IDMWorks

Special Thanks to JHU APL for providing the Parsons Auditorium for our use this evening
INNOVATION
leave it to us.

Business leadership demands best-of-breed technology. We believe that every business can be at its best, if their technology is at its best.
Identity & Access Management | Managed Services | Custom Application Development | Data Center Solutions

✓ Operational Since 2004
✓ Privately Owned
✓ D&B Rating of 95%
✓ 65+ 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 Sun & Passlogix), PingIdentity, Quest (Dell), RSA, Radiant Logic, Centrify & SailPoint
✓ Oracle Platinum Partner
✓ Net IQ Elite Partner
✓ Dell/Quest Elite Partner
✓ CA Elite Partner
✓ Hundreds of Successful Engagement with Clients Across Multiple Sectors

For more information please visit our website:

www.idmworks.com
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. – Gartner 2012
What is IDENTITY & ACCESS MANAGEMENT
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 & Control
Real-time enforcement of application security using identity-based, attribute based and policy based access controls and provisioned entitlements

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 Development
Success Approach

✓ Validate your current state
✓ Highlight your constraints
✓ Identify your crucial success factors
✓ Define your desired future state & first win
✓ Develop your blueprint
✓ Deliver a step by step roadmap:
  - Costs
  - Timelines
  - Milestones
  - Business Justification
Primary Focus of IAM

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

www.idmworks.com
As-Is (Current State)

User Adds Moves Deletes

Trouble Ticket System

Spreadsheet

Emails/Phone

Human Resources

Active Directory

Applications

Applications

Applications
Provisioning & Password Mgt

**WHY THIS DOESN’T WORK**
- Manual System Requires Multi-Steps
- Takes Weeks or Months
- No Audit Trail

Employee Adds Moves Deletes

Reports/ Audits

Trouble Ticket System

Spreadsheet

Emails

Human Resources

Active Directory

Applications

Applications

Applications

CONTACT US
510 Madeira Ave, Coral Gables, FL 33134
P. 888 687 0436 / info@idmworks.com

IDMWORKS
UNLEASH YOUR TRUE POTENTIAL
To-Be (Future State)

Provisioning & Password Management

Identity Management System

Human Resources

User Adds Moves Deletes

Reports/ Audits

WHY THIS WORKS

- Automated/self-service system
- Real time
- Includes audit trail

Active Directory

Applications

Applications

Applications

To - Be (Future State)
Assess environment and interview stakeholders to find gaps in “as-is” and “to-be” states

Form a team of Business Owners, IT Sec, Audit and Compliance

Focus on workflow and narrow the initial goal:
- Human or non-human
- Address mobile environment (BYOD)
- Areas that can be improved quickly

Gain Executive buy-in for funding by focusing on gains:
- Automate the account process: new, change, & remove for efficiency
- Improved speed to onboard
- Improve security on entitlement creep
- Improved audit on off-boarding
- Speed to deliver audit data
Validating access entitlements

User Adds Moves Deletes

Reports/Audits

Reports/Audits

Reports/Audits

Trouble Ticket System

Access Control

Access Governance

Spreadsheet

Emails

Human Resources

Active Directory

Applications

Applications

Applications

Automated Validation of Entitlements

Detective Attestation/Recertification

Automated Audit

HOW DO WE FIX THIS?
Preventative access entitlements

HOW DO WE PREVENT THIS?
- RBAC: Create Role
- ABAC: Define Attributes
- PBAC: Create Policies

User
- Adds
- Moves
- Deletes

Reports/Audits

Access Control
- Trouble Ticket System
- Spreadsheet
- Emails

Human Resources
- Active Directory
- Applications
- Applications
- Applications
Enforcement of access entitlements

Contact Us
510 Madeira Ave, Coral Gables, FL 33134
P. 888 687 0436 / info@idmworks.com

Access Control & Governance

AGS System
Prevent

Provisioning & Password Management
Identity Management System

Detect & Correct

Attestation

Reports/Audits

Reports/Audits

Human Resources
Active Directory
Applications
Applications
Applications

How have we fixed this? & How have we prevented this?
1) Automated Real-Time Changes
2) Policy Enforcement
3) Management Approvals
4) Audit Trail

Detect & Correct

Identity Management System
Assess environment and interview stakeholders to find key applications that require automation for improved compliance

Form team of Business Owners & IT Sec to define the ideal user experience (Employee and Manager)

Review & Enforce organizational policy around user accounts and PII:
- 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)
- GOVERNANCE!
Access to external apps

**As-Is** (Current State)

Every application requires integration to every external application for access.

**WHY THIS DOESN’T WORK**

- Manual Process Requires App Development
- Takes Weeks or Months
- No Common Control
- No Audit
Access to external apps

To-Be (Future State)

- System Adds Moves Deletes
- User Adds Moves Deletes

Single Sign On and Federation

WHY THIS WORKS
- Centralized Security
- Policy Enforcement
- Complete Audit Trail

www.idmworks.com
Success Approach

✓ Focus on the client
  ◦ Employee satisfaction around SSO
  ◦ Customer / Partner integration (ease of doing business)
✓ Assess the number of SAAS 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 to cloud initiatives
  ◦ HR
  ◦ CRM
  ◦ Supply chain
In addition to System Admins, Dbase Admins, Server Admins & Infra Admins... Every Non Human Applications Have Access to Systems Which Requires Manual Development & Audit

**WHY THIS DOESN’T WORK**
- Everyone has same access
- No audit
PRIVILEGED USER ACCESS

WHY THIS WORKS
✓ Can filter access
✓ Log usage and record suspicious activity
✓ Audit

System Admins
Developers
IT Admins

To-Be (Future State)

Privileged User Management
Password Vault
Session Record

Request

One-time use

Applications
Applications
Applications

CONTACT US
510 Madeira Ave, Coral Gables, FL 33134
P. 888 687 0436 / info@idmworks.com
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 orphans and exceptions
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 for your IAM roadmap?
✓ How are you communicating tangible and non-tangible 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 your IAM systems?
✓ How are you performing audit and compliance?
ASSESSMENT APPROACH

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