The Changing Landscape of State Government Identity Management

April 14, 2016

Michael Wyatt
Identity Services Solution Offering Leader
Deloitte & Touche LLP
Contents

• Cyber risk management
• The changing landscape of Identity Management
• The state of statewide Identity Management
• Case studies
• Final thoughts
Cyber Risk Management
We have connected our economy and society using platforms designed for sharing information… not protecting it

…and state agencies must trust people every day.
State Agencies Continue to be a Target

States collect, share, and use large volumes of the most comprehensive citizen information.

The large volume of information makes states an attractive target for both organized cyber criminals and hacktivists.
States Rapidly Embrace New Technology to Better Serve Constituents, Efficiently
The Innovations that Drive Growth also Create Cyber Risk

Threat actors exploit weaknesses that are byproducts of business growth and innovation.

- New citizen service models
- New sourcing and supply-chain models
- New applications and mobility tools
- Use of new technologies for efficiency gains and cost reduction

Perfect security is not feasible. Instead, reduce the impact of cyber incidents by becoming:

**SECURE** — Enabling business innovation by protecting critical assets against known and emerging threats across the state ecosystem

**VIGILANT** — Gaining detective visibility and preemptive threat insight to detect both known and unknown adversarial activity

**RESILIENT** — Strengthening your ability to recover when incidents occur

Cyber risk management is a positive aspect of managing business performance.
Identity Management
Identity & Access Management (IAM) Overview

The combination of both identity management and access management form the *identity services* layer of cyber security solutions.

**Identity Management**

- Organizations can construct a **trusted digital identity** for an individual or a device based on defining attributes.
- Identities may include not only employees and contractors but citizen, vendor and partner identities from third parties and social media sites as well.
- Identities may be provisioned with **entitlements** that allow the user to gain access to protected resources.

**Access Management**

- Organizations can **ensure only permitted individuals and systems are granted access** to protected resources.
- Access is granted to enterprise, cloud and third-party applications as well as non person identities and APIs.
- Permissions are granted through **authentication of trusted identities** and authorization of credentials, attributes, and assigned permissions.
The Digital Identity Lifecycle

A standard user lifecycle is typically followed by organizations who effectively use identity and access management services

1. An identity is created during the onboarding
2. Identity proofing builds trust in the identity
3. User credentials are established; authentication devices may be enrolled
4. Appropriate application access is established
5. User life cycle management
   - Access request / approvals
   - Status / Position change
   - Password reset
   Role life cycle management
   - Role assignment / approval
6. User access permissions are removed

Run-time Access management
- User authentication, MFA
- User authorization

Audit
- User access review / recertification
- Approver / Admin actions
Modern Drivers of Identity & Access Management

Five key drivers for the need for Identity & Access Management…

Deloitte’s POV on Drivers of IAM

- **Regulatory Compliance**: Ongoing regulatory compliance pressures and the need for an efficient identity governance process
- **Technology Trends**: Modern technology trends and increased adoption of social media, mobile, and cloud technologies are disruptive for enterprises
- **Cyber Risks**: Mitigation of cyber risks associated with data breaches, insider attacks, and malware
- **IT Complexity & Cost Efficiencies**: Need for reduced IT complexity and cost efficiency to maintain identity infrastructure and ongoing operations
- **User Experience**: Quality of user experience is the priority for consumer identity and mobile applications

…which increase in relevance in the modern technology landscape
Benefits of Identity Services

Significant value comes with an effectively deployed identity services architecture
Spotlight on Privileged Identity Management
Privileged Access Management

With nearly 40% of data breaches caused by misuse of privileged accounts, there is a need to proactively manage and monitor privileged access to information systems to prevent cyber attacks.

**CATALYST FOR TREND**

- Organizations need a *holistic approach to managing privileged access to critical infrastructure*
- Rather than granting permanent use, elevated privileges, privileges are granted on an as-needed basis, and actions taken with those privileges are closely monitored.

**BENEFITS PROVIDED**

- Privileged access management...
- ...Protection against insider threats to sensitive information
- ...Compliance with regulatory requirements
- ...Reduced risk from lost administrator passwords
- ...Traceability for malicious use

**CHALLENGES**

- Challenges with Privileged Access Management space include...
- ...Absence of privileged identity management in overall security scope
- ...Behavioral change for IT personnel
- ...Support for legacy applications and platforms

---

Regulatory Compliance  
Technology Trends  
Cyber Risks  
IT Complexity & Cost Efficiencies  
User Experience  

Modern Drivers
Who are Privileged Users?

On Premise

Employees/Partners
- Systems Admins
- Network Admins
  - DBAs
- Application Admins

Employees
- Systems/Network/DBA/Application administrators

Partners
- Systems/Network/DBA/Application Administrators

Office Suite / Productivity Software Administrator

AWS Administrator

Public Cloud

Internet

Hacker

Malware/APT
Privileged Account Management (PAM) Capabilities

IAM systems generally do not provide PAM capabilities since privileged identities/accounts are associated with hardware and software assets and not with the individual user identities controlled by IAM.

Privileged access control
- Control the use of shared accounts
- Total accountability for activities with privileged access
- Decrease insider threats

Securing critical application
- Centralized PAM
- Improves IT control and reduces risk
- Preventive control

Protecting sensitive assets
- Protection from advanced persistent threats
- Allow users temporary and/or time-limited use of super-user privileges
- Automated sign-on and check in/out simplifies usage

Active monitoring
- Broad tracking and reporting enhances accountability
- Ability to inspect and respond to suspicious activities
- Enable secure migrations

“The reality is that protection of privileged identities is a necessity not a luxury.”
Source: The Role of Privileged Accounts In High Profile Breaches by CyberSheath Services International, LLC, May 2014
PAM Implementation Approach

Our PAM implementation approach is designed to rapidly reduce security risk while minimizing operational risk.

**Discover**
- Discover the privileged identities by meeting with account owners, data mining identity management systems, and scanning the environment using a PAM discovery tool

**Design and Develop**
- Develop use cases for privileged accounts
  - Access control
  - Password management
- Map specific use cases to framework
- Configure account management structure in PAM solution

**Maintain and Enhance**
- Monitor account usage in PAM
- Develop process automation for PAM solution
- Threat Analytics: Analyze events using risk indicators and analyze trends over a period of time

**Implement**
- Deploy the PAM solution & on board privileged accounts
- Document and enforce the processes/policies associated with accessing privileged identities
- Educate the end users and administrators
Cloud and IDaaS
Digital Identity and Context in the Cloud

Two basic scenarios

**On-premise**
Extend Identity services capabilities to manage users and the resources they access outside the traditional enterprise.

**Cloud**
Use IDaaS / SaaS based IAM solutions that provide less flexibility but much of the value with less investment.

---

**Capital Expenditure**
- Software licenses
- Implementation & Customization
- Training
- IT Personnel
- Hardware Costs
- Maintenance

**Operational Expense**
- Subscription Fee
- Implementation & Customization
- Training

---

**On-going Costs**
- Apply fixes, patches and upgrades
- Performance Tuning
- Maintain & upgrade: hardware, Database, Security, etc.

**On-going Costs**
- Subscription fee
- Training
- Configuration
## Considerations of Premise/COTS vs. IDaaS

<table>
<thead>
<tr>
<th>Focus Points</th>
<th>On-Premise IdM</th>
<th>Cloud IdM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment</td>
<td>• Hardware, Software assessment &amp; purchasing</td>
<td>• Identity Vendor Assessment</td>
</tr>
<tr>
<td>Initial Setup – Hardware/Software</td>
<td>• Traditional implementation process - Analyze, Design, Build, Test, Performance Test (QA) and Production</td>
<td>• Simplified implementation process – Analyze, Design, Test &amp; Production</td>
</tr>
<tr>
<td></td>
<td>• Est. 2 – 3 months</td>
<td>• Est. 2 – 3 weeks</td>
</tr>
<tr>
<td>Customization – Custom Connectors and branding</td>
<td>• High number out of box connectors</td>
<td>• High number out of box connectors to choose from</td>
</tr>
<tr>
<td></td>
<td>• High ability to customize interfaces to meet organization requirements</td>
<td>• Limited interface customization</td>
</tr>
<tr>
<td></td>
<td>• Est. 4 – 12 months</td>
<td>• Est. 2 – 3 weeks</td>
</tr>
<tr>
<td>High Availability</td>
<td>• Requires additional Hardware to eliminate single point of failure</td>
<td>• Included as a part of IDaaS Vendor SLA</td>
</tr>
<tr>
<td></td>
<td>• Licensing for additional servers</td>
<td>• Vendor responsible for maintenance and uptime of environment(s)</td>
</tr>
<tr>
<td></td>
<td>• Binding resources to setup and manage Replication, Clustering &amp; Mirroring</td>
<td></td>
</tr>
<tr>
<td>Hardware, Software Security</td>
<td>• Typical process of downtime</td>
<td>• Completed by Vendor</td>
</tr>
<tr>
<td>updates and Maintenance</td>
<td>• Resource time to implement updates in Development, Test, Performance Test (QA) and Production</td>
<td>• Limited downtime</td>
</tr>
<tr>
<td>Cost</td>
<td>• Fixed Cost model</td>
<td>• Variable Cost model</td>
</tr>
<tr>
<td></td>
<td>• Potentially expensive due to variants in implementation &amp; setup</td>
<td>• Pay per use may be less expensive due to ability to scale out or downsize quickly and efficiently without paying high fix costs.</td>
</tr>
</tbody>
</table>
Case Studies

1. Commonwealth of Pennsylvania - Enterprise IAM
   URL: https://www.compass.state.pa.us/cwis/public/home

2. State of Michigan – MICAM
   URL: https://milogin.michigan.gov
Experience in implementing IAM for State benefits systems

<table>
<thead>
<tr>
<th>U.S State</th>
<th>IAM solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>State of Illinois</td>
<td>IBM</td>
</tr>
<tr>
<td>Commonwealth of Virginia</td>
<td>Oracle</td>
</tr>
<tr>
<td>State of Delaware</td>
<td>Oracle</td>
</tr>
<tr>
<td>State of Rhode Island</td>
<td>IBM</td>
</tr>
<tr>
<td>Commonwealth of Pennsylvania</td>
<td>CA</td>
</tr>
<tr>
<td>State of Georgia</td>
<td>CA</td>
</tr>
<tr>
<td>State of Montana</td>
<td>IBM</td>
</tr>
<tr>
<td>State of Alaska</td>
<td>IBM</td>
</tr>
<tr>
<td>State of Louisiana</td>
<td>Novell</td>
</tr>
</tbody>
</table>
Case study 1: Commonwealth of Pennsylvania– Enterprise IAM

Project Overview

Commonwealth of Pennsylvania (COPA) IAM program is an enterprise single sign-on and identity management solution which enables COPA to establish, manage, and authenticate user identities for various State Information Technology (IT) systems. The IAM program has been in place since 2002.

<table>
<thead>
<tr>
<th>Solution:</th>
<th>Centralized IAM solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target User population</td>
<td>~100k employees and contractors across 40+ COPA agencies ~3 Million (Citizens, 3rd party / Business partners)</td>
</tr>
<tr>
<td>Target Applications</td>
<td>60+ protected applications and increasing</td>
</tr>
</tbody>
</table>

COPA IAM at a Glance

Enterprise Provisioning
- Provisioning across 40+ agencies
- Used by 200+ agencies administrators

Enhanced User Experience
- Self-registration
- Forgotten password
- Request application access
- Update user’s profile

Business functionality
- Identity proofing
- Web services security
- Mobile applications
- Multi-factor authentication (MFA)

Compliance
- High Availability (HA)
- Complies with various Federal & State standards

Awards
- 2009: Winner of The Computerworld Honors Program
- 2012: Finalist in NASCIO State IT Recognition Awards

Solution Overview

COPA IAM services allow applications to enhance user experience, attain compliance, and reduce operational costs.
Case study 2: State of Michigan – MICAM Program

### Project Overview

<table>
<thead>
<tr>
<th>Solution:</th>
<th>Centralized IAM solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target User population</td>
<td>~5.5 Million (Citizens, 3rd party / Business partners, State staff, Other States)</td>
</tr>
<tr>
<td>Target Applications</td>
<td>395 applications (200 New Integrations and Migration of 195 applications)</td>
</tr>
</tbody>
</table>

### MICAM at a Glance

#### Enhanced User Experience
- Self-registration
- Self-service
- Password management
- Forgotten password
- Request application access
- Update user’s MICAM profile

#### Business functionality
- Identity proofing
- Enhanced security, e.g., supports Service-oriented architecture (SOA) based applications
- Mobile applications
- Multi-factor authentication (MFA)

#### Compliance
- High Availability (HA)
- Complies with various Federal & State standards
- Adheres to State’s accessibility & usability standards

### Solution Overview

MICAM services allow applications to enhance user experience, attain compliance, and reduce operational costs.

[Image of a table showing various MICAM services and features]

[Image of a diagram showing the architecture of MICAM services and enabling technology]
Why is MILogin Required?

A day in a life of an end user

MILogin allows end users to securely and seamlessly access the state’s various applications as well as the business partner applications, thus enabling better information sharing and enhancing privacy protection.
Transforming the State and Citizens’ Relationship

MILogin allows end users to securely and seamlessly access the state’s various applications as well as the business partner applications, thus enabling better information sharing and enhancing privacy protection.

- One customer – one set of credentials to access all State systems online.
- Added security measures such as multifactor authentication (MFA) and Identity Proofing for regulatory compliance and fraud prevention.
MiPage (State’s mobile initiative) user interface is built by leveraging the identity management and single sign-on engine provided by MILogin.

The MiPage mobile application is developed by the State’s eMichigan team and is available for download from Apple App Store and is also available for Android based phones.
Benefits of MILogin

MILogin services allow applications to enhance user experience, attain compliance, and reduce operational costs.

End User Experience
- Ease of navigation
- Seamless Access / Single Sign-On
- Security & Privacy
- Availability (24*7*365)
- Mobile Access

Regulations and Standards
- FISMA
- PCI DSS
- HITECH, HIPAA
- NIST, FIPS
- IRS 1075

MILogin
- Enhanced User Experience
  - Self-registration
  - Self-service
- Business functionality
  - Identity validation (you are who you say you are)
  - Enhanced security
  - Mobile applications
  - Multi-factor authentication (MFA)
- Compliance
  - Complies with various Federal & State standards
  - Adheres to State’s accessibility & usability standards
Final Thoughts

• IAM Program Governance

• Critical Success Factors
Identity Program Governance

Identity Program Governance is focused on establishing the elements necessary to effectively achieve IAM program vision through the alignment and coordination of disparate teams and activities.

Project Managers utilize specialized Program Resources to resolve questions and issues as appropriate.
With more than a decade of implementing IAM solutions for the State sector, Deloitte has identified critical success factors to roll out an IAM program, including the following:

<table>
<thead>
<tr>
<th>Critical Success Factors</th>
<th>Success Ingredients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>Organizational adoption and solution sustainability depends on establishment of an overarching governance framework and establishment of a strong support model.</td>
</tr>
<tr>
<td>Business Alignment</td>
<td>Business driven IAM helps deliver the IAM solution in line with the specific business needs increasing the support for program.</td>
</tr>
<tr>
<td>Bite size projects</td>
<td>Do not bite off more than you can chew. Define projects or phases that have clear metrics for success and that can be achieve in a decent amount of time.</td>
</tr>
<tr>
<td>A Solid IAM Architecture and Pilot</td>
<td>One that meets the comprehensive IAM requirements and displays business value.</td>
</tr>
<tr>
<td>Highly Experienced Team</td>
<td>One that meets your functional and technical requirements and demonstrates the potential of IAM at the client.</td>
</tr>
<tr>
<td>Collaboration and Staff Empowerment</td>
<td>Through collaboration and knowledge transfer to the client to own and independently maintain and operate the IAM environment.</td>
</tr>
</tbody>
</table>
Effectively Manage What is in Your Control

Being **SECURE** means having risk-prioritized controls to defend critical assets against known and emerging threats.

Being **VIGILANT** means having threat intelligence and situational awareness to anticipate and identify harmful behavior.

Being **RESILIENT** means being prepared and having the ability to recover from, and minimize the impact of, cyber incidents.
This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2016 Deloitte Development LLC. All rights reserved. Member of Deloitte Touche Tohmatsu Limited