1 Building an Identity Management Business Case

Managing the User Lifecycle Across On-Premises and Cloud-Hosted Applications

Justifying investment in identity management automation.

2 Agenda

- Business challenges due to managing identities, authentication factors and entitlements.
- Identity and access management (IAM) overview.
- IAM value proposition.
- Supporting metrics.
- Effective IAM projects.

3 Business Challenges
### 3.1 The user lifecycle

At a high level, the user lifecycle is essentially the same in all organizations and across all platforms.

### 3.2 IAM in silos

In most organizations, many processes affect many applications. This many-to-many relationship creates complexity:

- **Business processes**
  - Hire
  - Retire
  - Resign
  - Finish contract
  - Transfer
  - Fire
  - Start contract

- **IT processes**
  - New application
  - Retire application
  - Password expiry
  - Password reset

Systems and applications with users, passwords, groups, attributes
3.3 Access and credential challenges (1/2)

**For users**
- How to request a change?
- Who must approve the change?
- When will the change be completed?
- Too many passwords.
- Too many login prompts.

**For IT support**
- Onboarding, deactivation across many apps is challenging.
- More apps all the time!
- What data is trustworthy and what is obsolete?
- Not notified of new-hires/terminations on time.
- Hard to interpret end user requests.
- Who can request, who should authorize changes?
- What entitlements are appropriate for each user?
- The problems increase as scope grows from internal to external.

3.4 Access and credential challenges (2/2)

**For Security / risk / audit**
- Orphan, dormant accounts.
- Too many people with privileged access.
- Static admin, service passwords a security risk.
- Weak password, password-reset processes.
- Inappropriate, outdated entitlements.
- Who owns ID X on system Y?
- Who approved entitlement W on system Z?
- Limited/unreliable audit logs in apps.

**For Developers**
- Temporary access (e.g., prod migration).
- Half the code in every new app is the same:
  - Identify.
  - Authenticate.
  - Authorize.
  - Audit.
  - Manage the above.
- Mistakes in this infrastructure create security holes.

3.5 Business drivers for IAM

**Security / controls.**
- Reliable deactivation.
- Strong authentication.
- Appropriate security entitlements.

**Regulatory compliance.**
- PCI-DSS, SOX, HIPAA, EU Privacy Directive, etc.
- Audit user access rights.

**IT support costs.**
- Help desk call volume.
- Time/effort to manage access rights.

**Service / SLA.**
- Faster onboarding.
- Simpler request / approvals process.
- Reduce burden of too many login prompts and passwords.
3.6 IAM is linked to regulations

- Many regulations, in many jurisdictions, call for internal controls:
  - This implies effective AAA: Authentication, Authorization and Audit.
- Every system already has AAA.
  - The weakness is bad user/access data.
- The missing link is business process:
  - Appropriate access rights.
  - Timely access termination.
  - Effective authentication.
- Identity and access management process and technology are needed to bridge the gap between business requirements and AAA infrastructure.

4 IAM Overview

4.1 Identity and access management

Identity and access management is software to automate processes to securely and efficiently manage identities, entitlements and credentials:

<table>
<thead>
<tr>
<th>Processes:</th>
<th>Policies:</th>
<th>Connectors:</th>
</tr>
</thead>
</table>
| - Data synchronization.  
- Request portal.  
- Workflows to invite human participation.  
- Selection of approvers, reviewers and implementers.  
- Access reviews.  
- Segregation of duties.  
- Role-based access.  
- Risk scores.  
- Visibility, privacy. | - Applications.  
- Databases.  
- Operating systems.  
- Directories.  
- On-premises.  
- Cloud-hosted. |
4.2 Integrated IAM processes

Business processes
- Hire
- Retire
- Resign
- Finish contract
- Transfer
- Fire
- Start contract

IT processes
- New application
- Retire application
- Password expiry
- Password reset

Identity and Access Management System

Systems and applications with users, passwords, groups, attributes

4.3 Connecting users to applications

Identity and access management can be thought of as middleware for pulling security administration out of application silos.

5 IAM Value Proposition
5.1 IAM benefits

Identity and access management systems help organizations lower IT operating cost, improve user productivity and strengthen security:

<table>
<thead>
<tr>
<th>Security / compliance:</th>
<th>IT cost:</th>
<th>User service:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reliable, prompt and comprehensive deactivation.</td>
<td>• Reduce help desk, security admin workload and head count.</td>
<td>• Simplify change management.</td>
</tr>
<tr>
<td>• Policy enforcement: segregation of duties, role-based access.</td>
<td>• Simplify, streamline audits.</td>
<td>• Improve SLA – new hire, new access.</td>
</tr>
<tr>
<td>• Simplify entitlement audit and cleanup.</td>
<td></td>
<td>• Fewer passwords to remember, enter.</td>
</tr>
<tr>
<td>• Consistently strong authentication.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.2 Building a Business Case

An investment in identity and access management processes and infrastructure is normally supported by cost savings, improved productivity and stronger security:

<table>
<thead>
<tr>
<th>Cost savings</th>
<th>Productivity</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reassign staff out of the help desk or user administration group.</td>
<td>Help new users start work sooner and eliminate delays experienced by users who have problems or need changes.</td>
<td>Clean up entitlements, enforce security policies and create audit logs. Comply with SOX, GLB, HIPAA, etc.</td>
</tr>
</tbody>
</table>

Any business case should be supported by metrics:
- Current state.
- Desired outcome.

6 Supporting Metrics
## 6.1 Metrics: Password management

<table>
<thead>
<tr>
<th>Cost savings</th>
<th>Productivity</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Number of password problem help desk calls per month?</td>
<td>• Time spent by users before, during and after a typical password problem?</td>
<td>• How does the help desk authenticate callers?</td>
</tr>
<tr>
<td>• Cost and duration of each call?</td>
<td>• Value of wasted user time?</td>
<td>• Current vs. desired password policy on sensitive systems?</td>
</tr>
<tr>
<td>• Peak staffing to support post-weekend call volumes?</td>
<td></td>
<td>• Popularity of password “sticky notes?”</td>
</tr>
</tbody>
</table>

Example targets:

• Reduce password help desk calls by 75%.
• Reduce total help desk calls by 25%.
• Reduce passwords per user to 2.

## 6.2 Metrics: IAM

<table>
<thead>
<tr>
<th>Cost savings</th>
<th>Productivity</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Number of user add / change / deactivate operations per month?</td>
<td>• Number of different forms used to request new / changed access?</td>
<td>• SLA to terminate access for ex-employees? Ex-contractors?</td>
</tr>
<tr>
<td>• Cost and duration of each operation?</td>
<td>• Average time spent by users making requests (find the form, fill it out, send it to the right people, etc.)?</td>
<td></td>
</tr>
<tr>
<td>• Number of access security admin staff?</td>
<td>• IT SLA to fulfill valid, authorized requests?</td>
<td></td>
</tr>
</tbody>
</table>

Example targets:

• Reduce onboarding time from 3 days to 3 hours.
• Reduce admin FTEs from 6 to 2.
• Terminate access within 1 hour of departure.
6.3  **Metrics: Access certification**

**Cost savings**
- Cost of user access audits?
- Cost of excess software licenses?

**Security**
- Number of login accounts vs. number of real users?
- Security or regulatory exposure due to inappropriate entitlements?
- Total number of entitlements on integrated systems.
- Average number of entitlements per user.

6.4 **Metrics: Privileged access management**

<table>
<thead>
<tr>
<th><strong>Cost savings</strong></th>
<th><strong>Productivity</strong></th>
<th><strong>Security</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Person days to change passwords on all privileged accounts.</td>
<td>• Number of admin password changes per month.</td>
<td>• Number of privileged accounts per platform and total.</td>
</tr>
<tr>
<td>• Annual cost for production migrations because developers cannot be granted temporary access.</td>
<td>• Number of emergency admin access events per month.</td>
<td>• Number of systems per shared privileged account.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Time to deactivate terminated system administrators.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Time to determine what systems a departed administrator accessed before leaving.</td>
</tr>
</tbody>
</table>

Example targets:
- Time to deactivate administrator: 5 minutes.
- All admin passwords changed daily.

7 **Effective IAM Projects**
7.1 IAM project cost

License and maintenance for components:
• Directory.
• Meta-directory.
• Identity administration and access governance.
• Password management.
• Web, enterprise single signon (SSO).

Implementation services:
• Discovery, design.
• Installation, configuration.
• Testing, troubleshooting, user acceptance, pilot.
• User rollout.
• Incentives, user education and awareness.

Servers
• Hardware.
• Operating system license.
• Rack space.
• Support services.

Ongoing costs:
• System health monitoring.
• Adding features, integrations.
• User education, awareness.
• Ownership and coordination.

7.2 Minimizing deployment cost

<table>
<thead>
<tr>
<th>License model</th>
<th>Included tech.</th>
<th>Time savers</th>
<th>Efficient platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Simple $/user includes:</td>
<td>• Auto-discovery.</td>
<td>• Included web portal, request forms.</td>
<td>• Native code (EXE).</td>
</tr>
<tr>
<td>• All features:</td>
<td>• DB replication.</td>
<td></td>
<td>• Stored procs.</td>
</tr>
<tr>
<td>– Requests.</td>
<td>• Multi-master, active-active.</td>
<td>• Hitachi ID Identity Express.</td>
<td>• No J2EE or Sharepoint app server.</td>
</tr>
<tr>
<td>– Approvals.</td>
<td>• 120+ connectors.</td>
<td>• Policy-driven workflow.</td>
<td>• No separate products for workflow, reports, analytics, governance.</td>
</tr>
<tr>
<td>– Automation.</td>
<td>• Manual fulfillment.</td>
<td>• Self-service ID mapping.</td>
<td>• Works with existing directory.</td>
</tr>
<tr>
<td>– Certification.</td>
<td>• Proxy server.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
7.3 Change management: The human element

- Identity and access management can be political:
  - There are many stake-holders: application owners, security administrators, the help desk, audit, network operations, etc.
  - It's hard to get groups of people to agree on anything.
  - Executive sponsorship is essential to drive consensus.

- The user community must be involved:
  - Needs analysis.
  - Usability.
  - User training and awareness.
  - Incentives and dis-incentives.

- This is more about business process than technology:
  - How does your organization onboard new hires? manage change? terminate?
  - Business logic must capture authorization, login ID allocation, etc.

7.4 Getting an IAM project started

- Build a business case.
- Get management sponsorship and a budget.
- Discovery phase, capture detailed requirements.
- Assemble a project team:
  - security
  - system administration
  - user support
  - etc.

- Try before you buy: Demos, POCs, pilots.
- Install the software, roll to production.
- Enroll users, if/as required.