How to Establish a Business Case for Identity and Access Management

Andras Cser
Principal Analyst
Forrester Research

August 2010
Agenda

• Organizational ownership of IAM
• Selling IAM internally
• Assessing the drivers of IAM
• Quantifying the costs of IAM
• Quantifying the benefits of IAM
• Case study
Agenda

• Organizational ownership of IAM
• Selling IAM internally
• Assessing the drivers of IAM
• Quantifying the costs of IAM
• Quantifying the benefits of IAM
• Case study
Organization ownership of IAM

• Centralization is everywhere
• Consolidation of IAM product lines
• Usually IT Security or IT
• But we have seen:
  – CFO
  – Compliance
  – Application development
• Need at least 3-4 FTEs and budget upfront!
Organizational ownership

• This is the area where people struggle most
• Takes 6 months to design, implement and pilot an IAM project
• Takes 16 months to identify the organizational owner
• Be prepared for fights and budget increases
• Demonstrate value by going live with a phase every 3-4 months
Agenda

• Organizational ownership of IAM
• Selling IAM internally
• Assessing the drivers of IAM
• Quantifying the costs of IAM
• Quantifying the benefits of IAM
• Case study
Why IAM projects are problematic

- Ownership problems
- Usually no direct end user benefit
- Usually no front-office impact
- High product license cost
- Large integration effort and cost
- Extensive business and executive support needed
- Extensive times required
- Missed deadlines
- Difficult phasing and scoping

= NO PERCEIVED VALUE
Selling IAM internally

• Have a vision and presentation for executives
• Create metrics
• Track metrics as you implement
• Interview business people and get painpoints
• Scope small
• Implement to solve pain
• Track and document improvements in metrics
• Update the vision
Agenda

• Organizational ownership of IAM
• Selling IAM internally
• Assessing the drivers of IAM
• Quantifying the costs of IAM
• Quantifying the benefits of IAM
• Case study
Drivers and Benefits of IAM

- Security
- Compliance
- Business Agility
- IT Administration Efficiency
Security drives investment in IAM

“What is your firm's primary motivation for using identity and access management (IAM) within your enterprise?”

- Regulatory compliance: 15%
- Security: 49%
- Improving delivery of services to partners, customers, and/or employees: 17%
- Governance: 7%
- Cost reduction and worker productivity: 9%
- Don't know: 3%
- Improving delivery of services to partners, customers, and/or employees: 17%

Sample Size = 795 North American and European enterprise IT security decision-makers, whose firms are using IAM
Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2009
Single Sign-On and provisioning top list of IAM initiatives
“What are your firm's plans to adopt the following identity and access management (IAM) technologies?”

<table>
<thead>
<tr>
<th>IAM Initiative</th>
<th>Planning to implement in the next 12 months</th>
<th>Expanding/upgrading implementation</th>
<th>Implemented, not expanding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise/employee single sign-on (E-SSO)</td>
<td>14%</td>
<td>15%</td>
<td>16%</td>
</tr>
<tr>
<td>Web single sign-on/Web access management</td>
<td>12%</td>
<td>13%</td>
<td>16%</td>
</tr>
<tr>
<td>Provisioning (automated user account administration)</td>
<td>12%</td>
<td>11%</td>
<td>13%</td>
</tr>
<tr>
<td>Privileged user management</td>
<td>11%</td>
<td>8%</td>
<td>16%</td>
</tr>
<tr>
<td>Multifactor authentication</td>
<td>11%</td>
<td>8%</td>
<td>16%</td>
</tr>
<tr>
<td>Identity infrastructure consolidation</td>
<td>11%</td>
<td>8%</td>
<td>10%</td>
</tr>
<tr>
<td>Role design</td>
<td>10%</td>
<td>8%</td>
<td>11%</td>
</tr>
<tr>
<td>Consumer identity and access management...</td>
<td>8%</td>
<td>6%</td>
<td>10%</td>
</tr>
<tr>
<td>Federation</td>
<td>8%</td>
<td>5%</td>
<td>7%</td>
</tr>
<tr>
<td>Hosted/outsourced IAM</td>
<td>5%</td>
<td>1%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Sample Size = 1009 North American and European enterprise IT security decision-makers

Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2009
Agenda

• Organizational ownership of IAM
• Selling IAM internally
• Assessing the drivers of IAM
• Quantifying the costs of IAM
• Quantifying the benefits of IAM
• Case study
How to do a cost benefits analysis?

• Look at costs for 5 years
• Look at benefits for 5 years
License fees

- USD 15-25/internal user
- USD 2-5 / external user
- Connectors/Adapters: USD 15k/connected system
  - This is the biggest cost factor!!!
  - Reduce the number of repositories you have to provision to
  - Internalize skills to write connectors
- Software maintenance: 20-22% / year of initial license cost
External professional services

• USD 125/hr
• 1-2 resources
• 6 months
Internal labor

- Implementation 1 year
  - 3 FTEs
  - USD 70/FTE/hr

- Ongoing support
  - 5 FTEs
  - USD 50/FTE/hr
Hardware costs

• USD 50k / environment (middleware, DB, etc.)
• 3 environments
Agenda

• Organizational ownership of IAM
• Selling IAM internally
• Assessing the drivers of IAM
• Quantifying the costs of IAM
• Quantifying the benefits of IAM
• Case study
Onboarding new hires

• 10% turnover or growth of users
• USD 30 / hour / helpdesk person
• Manual time spent on onboarding a person: 1 hour
• 50% time saved at onboarding labor
Users performing self service – help desk labor reduction

• Users call the helpdesk twice a year

• 50% of them will use self service instead of calling helpdesk

• It costs about USD 5-8 / call
Users performing self service – enduser productivity improvements

• Users call the helpdesk twice a year

• When using self service, users will call the helpdesk once a year

• Users spend 10 minutes on the phone on each helpdesk call

• Hourly rate of users: USD 30/hr
Access requests and approvals and attestation

- 300 application owners (reviewers)
- 4000 managers (10% of total number of users) (reviewers)
- 16 hours saved per year per reviewer
- Reviewer average rate: USD 60/hour
- This is the biggest benefit factor!!!
Audit remediation avoided

- 10 audit findings without automated IAM
- Average cost for remediation: USD 12000/ finding
Detecting unused software licenses

• 5% of internal users don’t need to have access to at least one application

• Average license cost / seat: USD 30/seat
Potential cost for security breach

• 40k active and disabled users
• Remediation per user if records are lost: USD 30
• Probability of breach 10%
Agenda

• Organizational ownership of IAM
• Selling IAM internally
• Assessing the drivers of IAM
• Quantifying the costs of IAM
• Quantifying the benefits of IAM
• Case study
Case Study

• Multinational bank
• 134k users
• 12 connectors
• 12 FTE involved with IAM
<table>
<thead>
<tr>
<th></th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Costs</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License IAM for Internal users</td>
<td>2680000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License IAM for external users</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License IAM Connectors</td>
<td>180000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IAM Software maintenance</td>
<td>572000</td>
<td>572000</td>
<td>572000</td>
<td>572000</td>
<td>572000</td>
</tr>
<tr>
<td>External professional services</td>
<td>500000</td>
<td>500000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal labor: implementation</td>
<td>700000</td>
<td>700000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal labor: ongoing support</td>
<td>350000</td>
<td>525000</td>
<td>700000</td>
<td>700000</td>
<td>700000</td>
</tr>
<tr>
<td>Hardware</td>
<td>300000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total cost/year</strong></td>
<td>5282000</td>
<td>2297000</td>
<td>1272000</td>
<td>1272000</td>
<td>1272000</td>
</tr>
<tr>
<td><strong>Benefits</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Onboarding new hires</td>
<td>457275</td>
<td>685912.5</td>
<td>914550</td>
<td>914550</td>
<td>914550</td>
</tr>
<tr>
<td>Self-service - call center labor reduction</td>
<td>725543</td>
<td>108831.45</td>
<td>145108.6</td>
<td>145108.6</td>
<td>145108.6</td>
</tr>
<tr>
<td>Self-service - enduser productivity</td>
<td>217662.9</td>
<td>326494.35</td>
<td>435325.8</td>
<td>435325.8</td>
<td>435325.8</td>
</tr>
<tr>
<td>Access request and approvals</td>
<td>7517440</td>
<td>11276150</td>
<td>15034880</td>
<td>15034880</td>
<td>15034880</td>
</tr>
<tr>
<td>Audits avoided</td>
<td>125000</td>
<td>187500</td>
<td>250000</td>
<td>250000</td>
<td>250000</td>
</tr>
<tr>
<td>Recovering unused license fees</td>
<td>7200</td>
<td>10800</td>
<td>14400</td>
<td>14400</td>
<td>14400</td>
</tr>
<tr>
<td>Cost of security breach</td>
<td>402000</td>
<td>603000</td>
<td>804000</td>
<td>804000</td>
<td>804000</td>
</tr>
<tr>
<td><strong>Total benefit/year</strong></td>
<td>8799132.2</td>
<td>13198698.8</td>
<td>17598264</td>
<td>17598264</td>
<td>17598264</td>
</tr>
</tbody>
</table>

**Costs and Benefits**

**General**
- Internal users: 134000
- External users: 0
- Connectors: 12
- License cost USD/external user: 20
- License cost USD/external user: 0.2
- Cost per adapter USD: 15000
- Software maintenance cost % of license: 20
- Ext. preserve rate USD/hr: 125
- Int. implementation rate USD/hr: 70
- Int. ongoing support rate USD/hr: 50
- # of HW and SW environments: 6
- Machines per environment: 2
- Cost of one machine: 25000
- Implementation time ext. manhours: 4000
- Work hours in a year: 2000
- Implementation time int. manhours: 10000
- Ongoing support manhours/year: 14000
- Cost of remediation an audit finding USD / Finding: 10000
- Number of application owners: 24
- Number of managers: 13400
- Reviewer avg rate USD/hr: 70
- # of audit findings / year: 25
- User’s hourly pay rate USD/hr: 30
- Probability of a security breach: 20%
- Year 1 percentage of benefits realized: 50%
- Year 2 percentage of benefits realized: 75%
Thank you

Andras Cser
+1 617.613.6365
acser@forrester.com
www.forrester.com
Forrester and Novell

Novell® Identity Manager 4 Webcast III

Ben Goodman
Identity & Security
bgoodman@Novell.com
Novell Inc.
Agenda

Customer Challenges

Choosing An Identity Management Solution

Customer Success Story

Best Practices

Novell Identity Manager 4
Enterprises Face Challenges From All Sides
Identity And Access Management
The Key To Ensuring Policy Based Access

But How To Choose The Right Solution?
Value-Based Assessment
*Key To Choosing The Right Solution*

Key drivers to consider:

- IT Staff Efficiency Gains
- Business User Productivity Gains
- Operational Expense Savings
- Solution Deployment And Management Costs
- Compliance Certification Costs
- Cloud Security Costs
# Novell® Identity Manager

## Lower Costs And Improve Efficiency

<table>
<thead>
<tr>
<th>Without Identity Manager</th>
<th>With Novell® Identity Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>For 1 in 3 enterprises <strong>more than 40 percent</strong> of user access management is still <strong>manual</strong></td>
<td><strong>Automated timely access</strong> to resources improves user productivity and reduces dependence on IT</td>
</tr>
<tr>
<td>For 1 in 2 enterprises <strong>user's access revocation time</strong> is still <strong>more than one hour</strong></td>
<td><strong>Real-time automatic revocation</strong> of network access as soon as a user leaves an organization reduces IT management workload</td>
</tr>
<tr>
<td>For 1 in 3 enterprises <strong>more than 10 percent of IT resources</strong> are devoted to manual tasks such as <strong>compliance reporting</strong></td>
<td><strong>Automated reports</strong> on provisioning activity simplify audits by eliminating hundreds of hours of manual data collection and reports generation</td>
</tr>
</tbody>
</table>

Novell customer survey with infosurv around identity and security challenges - 2009

**Novell powered organizations move at the speed of business**
Novell® Identity Manager  
*Flexible Architecture That Supports The Cloud*

<table>
<thead>
<tr>
<th>Without Identity Manager</th>
<th>With Novell® Identity Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than <strong>20 percent of enterprises</strong> know who has access to appropriate resources</td>
<td><strong>Rich information on user access, privileges and provisioning activity</strong> to answer any GRC questions</td>
</tr>
<tr>
<td>By 2012, <strong>79 percent of CIO's</strong> will leverage the cloud but are <strong>unsure of data access and security</strong></td>
<td><strong>Enhanced security for cloud computing model</strong> through extension of enterprise policies to the cloud applications</td>
</tr>
<tr>
<td><strong>70 percent of enterprises</strong> want a single view across all systems to identity threats and violations</td>
<td><strong>Centralized point of control</strong> for unified policy based management across different systems – both on premise and in the cloud</td>
</tr>
</tbody>
</table>

**Novell powered organizations move at the speed of business**

Novell customer survey with infosurv around identity and security challenges - 2009
Western & Southern Financial Group
A Fortune 500 company with over $42B assets

“Novell offers a cost-effective, integrated suite of products across the entire identity management spectrum. Novell has a good vision for what we are trying to accomplish, and we found that Novell Access Governance Suite fills an important niche in the market.”

Mark W. Pfefferman, assistant vice president and director, Identity & Access Management

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase security to maintain superior reputation and support rapid growth rate without increasing headcount for additional reporting and support</td>
<td>Provided a robust identity foundation to provision access to systems and resources based on the user's role in the organization</td>
<td>Reduced the time spent on user provisioning by 80%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reduced password-related helpdesk calls by 45%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New users get network access their first day on the job</td>
</tr>
</tbody>
</table>
Synovus Financial
$33-billion dollar, multi-chartered financial services holding company

“We have a dynamic workforce. When a teller moves from one branch to another, for example, we needed a way to tie their credentials to their role so they could quickly get up and running. Now we’ve automated the entire user provisioning and deprovisioning processes, which now occur in near real time. So, when a user changes roles or moves from one location to another, all of their access rights are updated automatically.”

Steven Jones, Director of Operational Risk, Synovus Financial

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tighten access and security controls to satisfy bank regulators and 3rd party auditors, while reducing support costs</td>
<td>Provided compliance support with a robust identity foundation that reduced inactive accounts that could have been misused</td>
<td>Demonstrable compliance to Sarbanes-Oxley and other regulations like Gramm-Leach-Bliley, while cutting the associated IT costs by 80%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>40% reduction in password related help desk calls</td>
</tr>
</tbody>
</table>
Best Practices: Don’t Boil The Ocean

• Create a long term roadmap with short term achievable and quantifiable goals
• Define and contain project scope to manage expectations
• 80:20 rule: Start with most pressing areas where you get the biggest impact
• Build up your knowledge base as you expand your solution

A customer will reap benefits early on in the implementation process because of a well-planned identity management roadmap
Best Practices: Engagement Drives Success

- Identity management touches most of your enterprise systems
- Identify stakeholders crucial to project success
- Engage with all stakeholders early and often
- Iron-out ownership for data, policy and management
- Manage change – It is inevitable

A Novell customer with 40k users integrated 6 applications in 6 weeks because all stakeholders were highly engaged from the beginning
Moving To The Identity-Infused Enterprise
Novell® Identity Manager 4

Novell Identity Manager 4 is the only solution that securely manages identity and access across physical, virtual and cloud environments while reducing cost and ensuring compliance.
Useful Resources

Novell® Identity Manager
www.novell.com/identity

ROI study on Novell Identity Manager :

Novell® Identity Manager Flyer:
www.novell.com/idm4flyer

Novell® Identity Manager in action:
www.novell.com/products/identitymanager/launch/demos.html
Novell
Unpublished Work of Novell, Inc. All Rights Reserved.
This work is an unpublished work and contains confidential, proprietary, and trade secret information of Novell, Inc. Access to this work is restricted to Novell employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer
This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. Novell, Inc. makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for Novell products remains at the sole discretion of Novell. Further, Novell, Inc. reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.