Evolving Your Identity Management Program

Kelly Manthey

I&AM Practice Partner

solstice
CONSULTING

Brian Schlueter

Information Security Specialist–
Insurance Industry

Presentation Overview

- Today's Environment - Business Challenges
- The role of Identity Management (IdM) Solutions
- IdM Maturity Model
- Getting There: IdM Maturity Best Practices

Today's Environment is...

- Mergers & Acquisitions
- Re-Organizations
- Security Breaches
- Regulatory Agency Requirements
- Doing More with Less

Organization Impact: A constant state of change

| Mergers and Acquisition	• On-boarding and off-boarding employees • Merging business processes
Enterprise Re-Orgs	• Job function changes • Changes to system access needs
Security Breaches	• Accountability for system access controls • Need for system access audits • Need for rapid response
Regulatory Expectations	• Identification and implementation of proper controls
Do More with Less	• Budgets are tight • Need to reduce administrative overhead

An Identity Management Solution
Helps Manage Change

- Identity Management is……
  - credential management
  - Management of user access to technology assets (HW, SW, services)
  - the reduction of usernames and passwords
  - tying usernames/passwords to real people
  - a defined and repeatable process for the requesting and granting of system access
  - accountability for the scheduled review of access

Access Request → Approvals → Provisioning → Certification

An Identity Management Solution Helps Manage Change

- Getting people the **right information** at the right time to do their jobs
- **Consistency** in the granting of system access
- **Automation** of the administrative overhead associated with granting system access
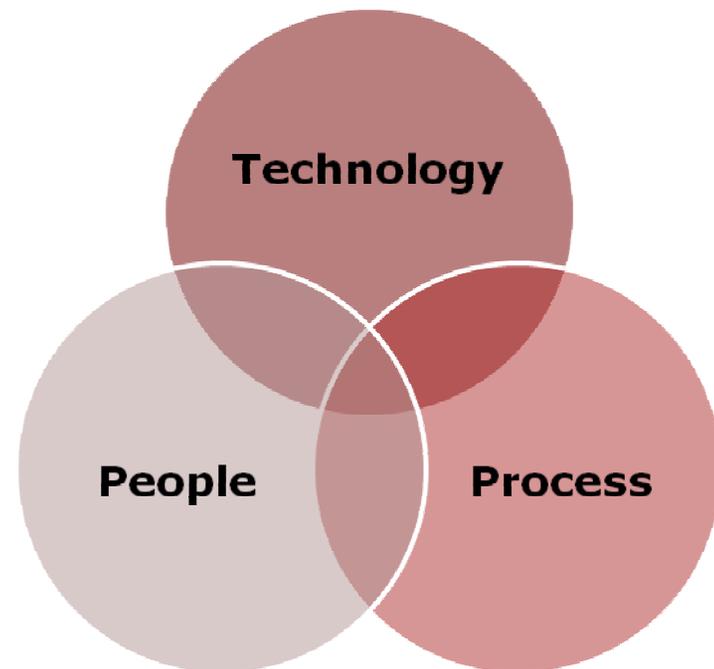
Selling the Benefits in $$

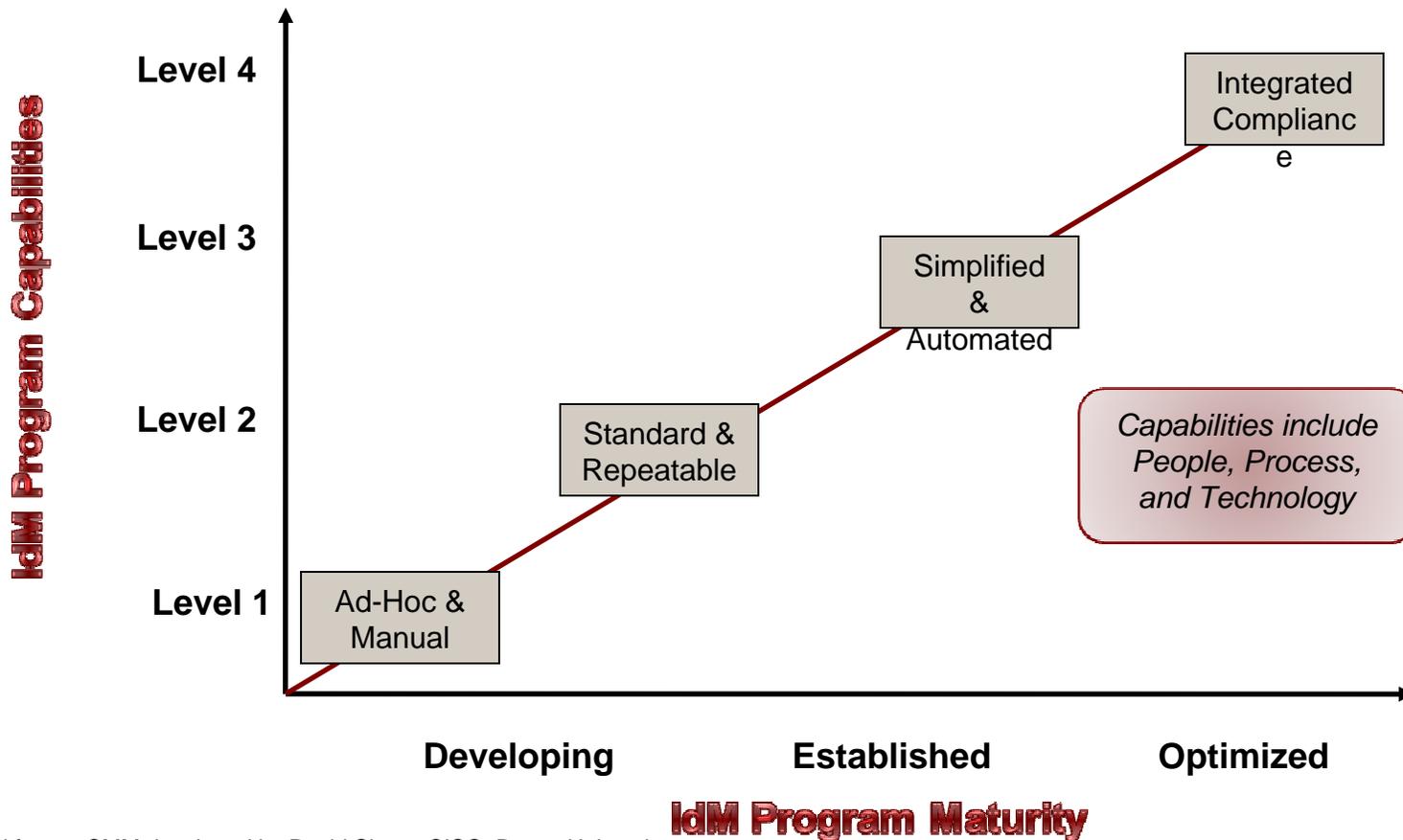| Efficiency	Compliance	Security
• Faster account set-ups through workflow based provisioning • Reduction in workforce involvement in account creation • Reduction in call center/help desk volumes	• Cost of generating audit reports • Cost of remediating audit findings • Segregation of Duties violations; each violation represents fiscal risk	• Reduction in orphan account clean-up/administration • Reduction in Segregation of Duties violations • Administration of separate IDs/passwords for one user

Source: Forrester Research

Capability Maturity Model

IdM Program Capabilities (vertical axis)

- Level 4 — Integrated Compliance
- Level 3 — Simplified & Automated
- Level 2 — Standard & Repeatable
- Level 1 — Ad-Hoc & Manual

Capabilities include People, Process, and Technology

IdM Program Maturity (horizontal axis): Developing — Established — Optimized

Adapted from a CMM developed by David Sherry CISO, Brown University

Getting There: Developing

- Make IDM a strategic priority
- Educate
- Define your Access Request process/roles & responsibilities
- Involve stakeholders

- Identify authoritative source(s)

Getting There: Established

- Establish oversight
- Determine information owners
- Role definition and management model

- Develop a standard company architecture
- Evaluate automation tools

Identity Management Vendor Landscape

- Major Players
  - Oracle, Sun, IBM, CA, Novell
- The IdM technology space has matured
- Frameworks are standardized
- Go with the vendor you like/are most comfortable working with

Getting There: Optimized

- Delegated responsibility
- Enterprise role management roadmap

- Align your architecture with open standards
- Enterprise Role Management automation tool evaluation

Closing Thoughts

- Educate
- Focus on all three aspects
  - People, Process, & Technology
- Define a roadmap; Don't try to do it all upfront
- Start simple; accomodate complexity as your maturity grows

Contact Us:

Kelly Manthey solstice CONSULTING

p: 312-371-9765

e: kmanthey@solstice-consulting.com

Brian Schlueter

p: 312-206-5380

e: br.schlueter@gmail.com